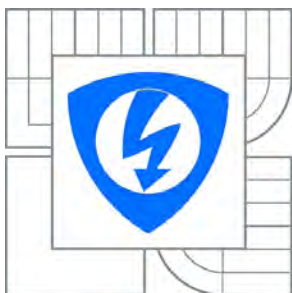




VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH  
TECHNOLOGIÍ

ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION  
DEPARTMENT OF TELECOMMUNICATIONS

## LABORATORNÍ ÚLOHY V PROSTŘEDÍ OPNET PRO PŘEDMĚT KOMUNIKAČNÍ TECHNOLOGIE

LABORATORY EXERCISES IN OPNET ENVIRONMENT FOR COMMUNICATION TECHNOLOGIES  
COURSE

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

AUTOR PRÁCE

AUTHOR

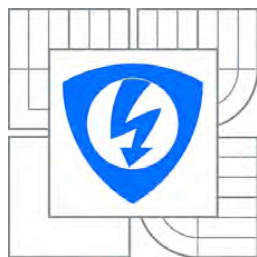
Bc. ROBIN KASPER

VEDOUCÍ PRÁCE

SUPERVISOR

Ing. JAN JEŘÁBEK, Ph.D.

BRNO 2012



VYSOKÉ UČENÍ  
TECHNICKÉ V BRNĚ

Fakulta elektrotechniky  
a komunikačních technologií

Ústav telekomunikací

# Diplomová práce

magisterský navazující studijní obor  
**Telekomunikační a informační technika**

**Student:** Bc. Robin Kasper

**ID:** 111067

**Ročník:** 2

**Akademický rok:** 2011/2012

## NÁZEV TÉMATU:

**Laboratorní úlohy v prostředí OPNET pro předmět Komunikační technologie**

## POKYNY PRO VYPRACOVÁNÍ:

Seznamte se s obsahem předmětu Komunikační technologie. V rámci diplomové práce navrhnete a zpracujete 4 úlohy pro prostředí OPNET tak, aby byly funkční ve verzi IT Guru. Vytvořte ke každé úloze i vzorové řešení a návod k řešení pro studenty. Úlohy musí v širším rámci spadat do obsahu předmětu a délkou musí odpovídat tříhodinovému cvičení předmětu. Zaměřte se především na témata, jako jsou srovnání různých fyzických technologií, protokolů UDP a TCP a také srovnání různých směrovacích protokolů.

## DOPORUČENÁ LITERATURA:

- [1] JEŘÁBEK, J. Pokročilé komunikační techniky, Skriptum FEKT VUT v Brně, 248 stran, 2011.
- [2] FOROUZAN, B. A. TCP/IP Protocol Suite, McGraw-Hill Higher Education, Boston, 4. vydání, 979 stran, 2010.
- [3] OPNET Technologies, OPNET Modeler Product Documentation Release 16.0, 2010.

**Termín zadání:** 6.2.2012

**Termín odevzdání:** 24.5.2012

**Vedoucí práce:** Ing. Jan Jeřábek, Ph.D.

**Konzultanti diplomové práce:**

**prof. Ing. Kamil Vrba, CSc.**

*Předseda oborové rady*

## UPOZORNĚNÍ:

Autor diplomové práce nesmí při vytváření diplomové práce porušit autorská práva třetích osob, zejména nesmí zasahovat nedovoleným způsobem do cizích autorských práv osobnostních a musí si být plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č.40/2009 Sb.

## **ABSTRAKT**

Tato diplomová práce se zabývá návrhem laboratorních úloh pro předmět Komunikační technologie, který je zařazen do druhého ročníku bakalářského studia oboru Teleinformatika. Předmět představuje první seznámení studentů se síťovými protokoly a technologiemi, proto se práce zabývá právě základními fyzickými technologiemi, směrovacími protokoly a protokoly transportní vrstvy.

Úvodní část práce je věnována teoretickým znalostem k jednotlivým úlohám. K návrhu laboratorních úloh je využito prostředí OPNET, konkrétně jeho neplacená verze IT Guru Academic Edition 9.1. První úloha je orientována na rozdíly u dvou základních transportních protokolů *Transmission Control Protocol* (TCP) a *User Datagram Protocol* (UDP). Další úloha je zaměřena na rozdíly přenosových parametrů sítě při použití bezdrátové sítě a technologie Ethernet. V třetí úloze jsou srovnávány směrovací protokoly *Routing Information Protocol* (RIP) a *Open Shortest Path First* (OSPF). Jedná se tedy o protokoly skupiny *Interior Gateway Protocol* (IGP), které jsou charakteristické použitím uvnitř jednoho autonomního systému. Poslední navržená úloha je zaměřena na technologie *Asynchronous Transfer Mode* (ATM) a Frame Relay, což jsou technologie používané převážně v sítích *Wide Area Network* (WAN).

Ke všem navrženým úlohám byl vypracován podrobný návod pro studenty včetně doplňujících otázek a úkolů vedoucích k samostatné práci a zamyšlení. K úlohám bylo vypracováno vzorové řešení a na přiložené CD vloženy zdrojové kódy programů.

## **KLÍČOVÁ SLOVA**

OPNET, IT Guru, laboratorní úloha, technologie, protokol

## **ABSTRACT**

This master's thesis deals with the design of laboratory exercises for the Communication Technologies course that is included in the second year of bachelor's degree in Teleinformatics. This course represents first introduction of students with network protocols and technologies, therefore, the thesis deals with just the basic physical technologies, routing protocols and transport layer protocols.

The introductory part of the thesis is devoted to theoretical knowledge to particular tasks. For the design of laboratory exercises is used OPNET environment, concretely its unpaid version

IT Guru Academic Edition 9.1. The first task is focused on the differences in two basic transport protocols *Transmission Control Protocol (TCP)* and *User Datagram Protocol (UDP)*. The second task is orientated on the differences in the transmission network parameters using wireless networks and Ethernet technologies. In the third task the routing protocols *Routing Information Protocol (RIP)* and *Open Shortest Path First (OSPF)* are compared. These are protocols of a group *Interior Gateway Protocol (IGP)* that are characterized by the usage within a single autonomous system. The last exercise is aimed at *Asynchronous Transfer Mode (ATM)* and Frame Relay technologies, which are technologies used mainly in networks *Wide Area Network (WAN)*.

All devised exercises are accompanied by detailed instructions for students including supplementary questions and tasks leading to individual work and reflection. The thesis includes model solutions to these four exercises and CD where are inserted all programs source codes.

## **KEYWORDS**

OPNET, IT Guru, laboratory exercise, technology, protocol

KASPER, R. *Laboratorní úlohy v prostředí OPNET pro předmět Komunikační technologie*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2012. 165 s. Vedoucí diplomové práce Ing. Jan Jeřábek, Ph.D..

## PROHLÁŠENÍ

Prohlašuji, že svou diplomovou práci na téma „Laboratorní úlohy v prostředí OPNET pro předmět Komunikační technologie“ jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené diplomové práce dále prohlašuji, že v souvislosti s vytvořením této diplomové práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

V Brně dne .....

.....  
podpis autora

## PODĚKOVÁNÍ

Děkuji vedoucímu mé diplomové práce Ing. Janu Jeřábkoví, Ph.D., za velmi užitečnou metodickou pomoc a cenné rady při zpracování práce.

V Brně dne .....

.....

podpis autora

Výzkum popsáný v této diplomové práci byl realizován v laboratořích podpořených z projektu SIX; registrační číslo CZ.1.05/2.1.00/03.0072, operační program Výzkum a vývoj pro inovace.



# OBSAH

<b>Seznam obrázků</b>	<b>12</b>
<b>Seznam tabulek</b>	<b>16</b>
<b>Úvod</b>	<b>17</b>
<b>1 Prostředí IT Guru</b>	<b>18</b>
1.1 Seznámení s prostředím IT Guru .....	18
1.2 Project editor .....	18
1.2.1 Hlavní menu .....	19
1.2.2 Oblast ikon .....	20
1.2.3 Pracovní plocha .....	20
1.2.4 Textová oblast .....	20
1.2.5 Tipy .....	21
<b>2 Transportní protokoly</b>	<b>22</b>
2.1 User Datagram Protocol (UDP) .....	22
2.2 Transmission Control Protocol (TCP) .....	23
<b>3 Přenosové technologie</b>	<b>26</b>
3.1 Wireless Local Area Network (WLAN) .....	26
3.1.1 CSMA/CA .....	26
3.2 Ethernet .....	27
3.2.1 CSMA/CD .....	27
3.2.2 Verze Ethernetu .....	28
<b>4 Protokoly pro sítě typu Wide Area Network (WAN)</b>	<b>30</b>
4.1 Asynchronous Transfer Mode (ATM) .....	30
4.1.1 ATM síťová vrstva .....	30
4.1.2 ATM adaptační vrstva .....	31
4.2 Frame Relay .....	32
4.2.1 Typy síťových zařízení .....	32
4.2.2 Virtuální okruhy .....	33
<b>5 Směrovací protokoly</b>	<b>34</b>

5.1	Routing Information Protocol (RIP) .....	34
5.1.1	Bellmanův-Fordův algoritmus .....	34
5.1.2	Verze protokolu RIP .....	35
5.1.3	RIPv2 paket .....	35
5.2	Open Shortest Path First (OSPF) .....	36
5.2.1	OSPF oblasti .....	37
5.2.2	Dijkstrův algoritmus .....	37
5.2.3	Verze OSPF .....	37
5.2.4	OSPF paket .....	38
5.3	Shrnutí ke směrovacím protokolům .....	39
<b>6</b>	<b>Laboratorní úlohy</b>	<b>40</b>
<b>7</b>	<b>Srovnání protokolů TCP a UDP</b>	<b>42</b>
7.1	Úvod k laboratorní úloze .....	42
7.2	Úkol 1 – vytvoření topologie .....	42
7.2.1	Popis vytvoření programu .....	42
7.2.2	Doplňující otázky a úkoly .....	54
7.3	Úkol 2 – navazování spojení .....	55
7.3.1	Postup .....	55
7.3.2	Doplňující otázky a úkoly .....	57
7.4	Úkol 3 – zahazování paketů .....	57
7.4.1	Postup .....	57
7.4.2	Doplňující otázky a úkoly .....	60
<b>8</b>	<b>Srovnání WLAN s Ethernetem</b>	<b>62</b>
8.1	Úvod k laboratorní úloze .....	62
8.2	Úkol 1 – vytvoření topologie .....	62
8.2.1	Popis vytvoření programu .....	62
8.2.2	Doplňující otázky a úkoly .....	71
8.3	Úkol 2 – parametry WLAN v závislosti na vzdálenosti .....	71
8.3.1	Postup .....	72
8.3.2	Doplňující otázky a úkoly .....	76
8.4	Úkol 3 – rozšíření topologie .....	76
8.4.1	Postup .....	76
8.4.2	Doplňující otázky a úkoly .....	80

<b>9</b>	<b>Směrovací protokoly</b>	<b>81</b>
9.1	Úvod k laboratorní úloze .....	81
9.2	Úkol 1 – vytvoření topologie, simulace RIP.....	81
9.2.1	Popis vytvoření programu.....	81
9.2.2	Doplňující otázky a úkoly .....	91
9.3	Úkol 2 – rozšíření o nové scénáře s OSPF.....	92
9.3.1	Postup.....	92
9.3.2	Doplňující otázky a úkoly .....	97
9.4	Úkol 3 – nastavení výpadku linky .....	99
9.4.1	Postup.....	99
9.4.2	Doplňující otázky a úkoly .....	102
<b>10</b>	<b>Technologie ATM a Frame Relay</b>	<b>104</b>
10.1	Úkol 1 - ATM .....	104
10.1.1	Popis vytvoření programu.....	104
10.1.2	Doplňující otázky a úkoly .....	121
10.2	Úkol 2 – Frame Relay .....	122
10.2.1	Postup.....	123
10.2.2	Doplňující otázky a úkoly .....	129
	<b>Závěr</b>	<b>130</b>
	<b>Literatura</b>	<b>131</b>
	<b>Seznam použitých zkratk</b>	<b>133</b>
	<b>Seznam příloh</b>	<b>135</b>
<b>A</b>	<b>Řešení pro srovnání protokolů TCP a UDP</b>	<b>136</b>
<b>B</b>	<b>Řešení pro srovnání WLAN s Ethernetem</b>	<b>142</b>
<b>C</b>	<b>Řešení pro Směrovací protokoly</b>	<b>150</b>
<b>D</b>	<b>Technologie ATM a Frame Relay</b>	<b>157</b>
<b>E</b>	<b>Obsah přiloženého CD</b>	<b>166</b>

# SEZNAM OBRÁZKŮ

Obr. 1.1: Okno project editoru v prostředí IT Guru.....	19
Obr. 1.2: Položky menu v IT Guru. ....	20
Obr. 1.3: Oblast ikon v project editoru prostředí IT Guru. ....	20
Obr. 1.4: Textová oblast programu IT Guru. ....	20
Obr. 1.5: Zobrazení kontextové nápovědy.....	21
Obr. 2.1: UDP datagram. [13].....	22
Obr. 2.2: TCP segment. [15].....	23
Obr. 4.1: ATM buňka. ....	30
Obr. 4.2: Identifikátory ATM spoje.....	31
Obr. 4.3: Formát rámce Frame Relay. ....	32
Obr. 5.1: Paket RIPv2. ....	35
Obr. 5.2: OSPF paket.....	38
Obr. 7.1: Základní topologie úlohy.....	43
Obr. 7.2: Podsít' serveru.....	44
Obr. 7.3: Klientská podsít'. ....	44
Obr. 7.4: Propojení IP_cloud a směrovačů technologií DS3.....	45
Obr. 7.5: Nastavení komponenty Task. ....	46
Obr. 7.6: Nastavení vlastní aplikace v <i>Manual Configuration</i> . ....	46
Obr. 7.7: Definice síťového provozu. ....	46
Obr. 7.8: Definice aplikace v okně <i>Application Config</i> .....	47
Obr. 7.9: Nastavení vlastní ( <i>custom</i> ) aplikace.....	48
Obr. 7.10: Nastavení parametrů profilu pro aplikaci. ....	49
Obr. 7.11: Nastavení parametrů simulace.....	51
Obr. 7.12: Ukázka okna výsledků.....	52
Obr. 7.13: Detail statistiky pro vlastní aplikaci v bajtech/s. ....	52
Obr. 7.14: Nastavení UDP protokolu pro aplikaci.....	53
Obr. 7.15: Nastavení UDP protokolu ve vlastní ( <i>custom</i> ) aplikaci. ....	54
Obr. 7.16: Nastavení parametrů v <i>Manage Scenarios</i> . ....	54
Obr. 7.17: Duplikování scénáře. ....	55

Obr. 7.18: Nastavení nového spojení pro každý požadavek.....	56
Obr. 7.19: Nastavení parametrů v <i>Manage Scenarios</i> .....	56
Obr. 7.20: Nastavení zdrojových dat. ....	58
Obr. 7.21: Nastavení zahazování paketů. ....	59
Obr. 7.22: Okno <i>Manage Scenarios</i> . ....	59
Obr. 7.23: Výsledný graf propustnosti na lince směrem od serveru k IP_cloud v bitech/s. ....	60
Obr. 8.1: Základní topologie.....	63
Obr. 8.2: Podsít' serveru.....	64
Obr. 8.3: Podsít' klienta.....	64
Obr. 8.4: Okno výběru prvků pro propojení prvků v podsítích. ....	65
Obr. 8.5: Nastavení aplikace FTP.....	65
Obr. 8.6: Nastavení profilu pro aplikaci FTP. ....	66
Obr. 8.7: Podpora aplikace na serveru ( <i>Supported Services</i> ). ....	66
Obr. 8.8: Nastavení parametrů simulace.....	67
Obr. 8.9: Ukázka statistiky pro odeslaná data FTP v paketech/s.....	68
Obr. 8.10: Podsít' bezdrátového klienta. ....	69
Obr. 8.11: Nastavení přístupového bodu. ....	69
Obr. 8.12: Propojení přístupového bodu s přepínačem. ....	70
Obr. 8.13: Nastavení parametrů simulace.....	71
Obr. 8.14: Nastavení VoIP aplikace. ....	72
Obr. 8.15: Nastavení profilu pro VoIP aplikaci.....	73
Obr. 8.16: Nastavení podpory profilu VoIP na serveru.....	73
Obr. 8.17: Nastavení klienta. ....	74
Obr. 8.18: Spuštění simulace. ....	75
Obr. 8.19: Celkové zpoždění u WLAN a Ethernetu v s/min. ....	75
Obr. 8.20: Rozšířená podsít' serveru.....	77
Obr. 8.21: Rozšířená podsít' klientů.....	77
Obr. 8.22: Přidání HTTP aplikace. ....	78
Obr. 8.23: Nastavení/přidání HTTP profilu.....	78
Obr. 8.24: <i>Manage Scenarios</i> .....	80
Obr. 9.1: Základní topologie úlohy bez propojení.....	82
Obr. 9.2: Podsít' Praha. ....	83
Obr. 9.3: Kompletní topologie úlohy.....	84

Obr. 9.4: Podsít' Brno včetně spoje ke směrovači 8. ....	85
Obr. 9.5: Nastavení IP adres pro směrovač Praha_hlavni. ....	86
Obr. 9.6: Nastavení statistiky RIP. ....	86
Obr. 9.7: Nastavení parametrů simulace. ....	87
Obr. 9.8: Ukázka topologie s vepsanými IP adresami, které mohou být odlišné. ....	88
Obr. 9.9: Směrovací tabulka pro směrovač Praha_hlavni. ....	89
Obr. 9.10: Statistika celkového RIP provozu v síti v bitech/s. ....	89
Obr. 9.11: Nastavení parametrů pro RIPv2. ....	90
Obr. 9.12: Změna nastavení masek u směrovače Praha_hlavni. ....	91
Obr. 9.13: Metriky jednotlivých spojů. ....	93
Obr. 9.14: Nastavení metriky pro vybrané spoje. ....	93
Obr. 9.15: Nastavení směrovacího protokolu OSPF. ....	94
Obr. 9.16: Konfigurace IP provozu mezi směrovači 1 a 6. ....	94
Obr. 9.17: Statistika OSPF provozu v topologii bez oblastí v bitech/s. ....	95
Obr. 9.18: Konfigurace jednotlivých oblastí. ....	96
Obr. 9.19: Vizualizace oblastí. ....	96
Obr. 9.20: Topologie s nastavenými a vizualizovanými oblastmi. ....	97
Obr. 9.21: Zobrazení nastaveného IP provozu mezi směrovači. ....	98
Obr. 9.22: Výpis cesty mezi směrovači 1 a 6 pro scénář OSPF_bez_oblasti. ....	99
Obr. 9.23: Nastavení výpadku a obnovení spoje. ....	100
Obr. 9.24: Nastavení exportu směrovací tabulky v různých časech. ....	101
Obr. 9.25: Simulování scénářů pomocí Manage Scenarios. ....	101
Obr. 9.26: Výběr požadovaných scénářů u možnosti Select Scenarios. ....	103
Obr. 9.27: Celkový OSPF provoz v síti s oblastmi i bez oblastí s výpadkem linky v bitech/s. ....	103
Obr. 10.1: Základní topologie bez propojení. ....	106
Obr. 10.2: Nastavení názvu a adresy pro klienta FTP. ....	106
Obr. 10.3: Propojení topologie spojem ATM_adv. ....	107
Obr. 10.4: Hromadné nastavení linky na přenosovou rychlost DS1. ....	108
Obr. 10.5: Nastavení aplikací a jejich parametry. ....	109
Obr. 10.6: Nastavení profilu pro aplikaci FTP. ....	110
Obr. 10.7: Nastavení profilu pro aplikaci EMAIL. ....	110
Obr. 10.8: Nastavení profilu pro aplikaci VOICE. ....	111
Obr. 10.9: Podpora aplikace na serveru ( <i>Supported Services</i> ). ....	112

Obr. 10.10: Nastavení třídy služeb ABR na serveru FTP.....	112
Obr. 10.11: Nastavení podpory serveru pro klienta FTP.....	113
Obr. 10.12: Nastavení třídy služeb CBR na přepínačích.....	115
Obr. 10.13: Nastavení parametrů simulace.....	117
Obr. 10.14: Ukázka okna se statistikami pro úvodní scénář.....	118
Obr. 10.15: Nastavení třídy služeb UBR. ....	119
Obr. 10.16: Nastavení parametrů simulace.....	120
Obr. 10.17: Ukázka statistiky <i>Download Response Time (sec)</i> pro FTP aplikaci. ....	120
Obr. 10.18: Nastavení provozu na pozadí na spoji mezi přepínači. ....	121
Obr. 10.19: Nastavení zvýšené zátěže pro aplikace FTP a EMAIL. ....	122
Obr. 10.20: Základní topologie pro Frame Relay.....	124
Obr. 10.21: Nastavení názvů PVC spojů. ....	125
Obr. 10.22: Určení typu provozu <i>Best Effort (0)</i> . ....	126
Obr. 10.23: Nastavení PVC pro best_effort.....	126
Obr. 10.24:Nastavení PVC pro excellent_effort.....	127
Obr. 10.25: Nastavení PVC pro interactive_voice. ....	127
Obr. 10.26: Zpoždění pro hlasovou aplikaci v s/min.....	128
Obr. 10.27: Nastavení třídy <i>Best Effort</i> pro hlasovou aplikaci. ....	128

# SEZNAM TABULEK

Tab. 1.1: Popisky k funkcím ikon.....	20
Tab. 3.1: Srovnání WLAN standardů. ....	27
Tab. 3.2: Přenosové rychlosti, standardy a verze Ethernetu. [9], [14].....	29
Tab. 9.1: IP adresy směrovačů pro připojení simulovaných LAN sítí. ....	85



# ÚVOD

Cílem diplomové práce je návrh laboratorních úloh pro předmět Komunikační technologie. Předmět je ve studijním plánu zařazen do třetího semestru bakalářského programu a studentům poskytne první seznámení se sítovými technologiemi v rámci studia oboru Teleinformatiky (TLI). V navržených úlohách se proto studenti seznámí se základními sítovými protokoly a přenosovými technologiemi. Pro návrh a simulaci bude využit program IT Guru Academic Edition 9.1 od společnosti OPNET Technologies, Inc.

Úvodní část této práce bude zaměřena na popsání použitého simulačního prostředí IT Guru Academic Edition 9.1, včetně popsání jednotlivých částí programu. Navržené laboratorní úlohy budou zaměřeny na protokoly transportní vrstvy, přenosové technologie a směrovací protokoly. Teoretická část práce se proto bude věnovat popisu transportních protokolů Transmission Control Protocol (TCP) a User Datagram Protocol (UDP), přenosových technologií Wireless Local Area Network (WLAN), Ethernet, Asynchronous Transfer Mode (ATM) a Frame Relay a směrovacích protokolů Routing Information Protocol (RIP) a Open Shortest Path First (OSPF).

V práci bude dále vypracován detailní návrh čtyř laboratorních úloh zaměřených právě na sítové technologie a protokoly popsané v teoretické části práce. Úlohy budou koncipovány tak, aby studentům poskytly vhodnou pomůcku pro pochopení dané problematiky. Každá z navržených úloh bude zaměřena na dvě sítové technologie či dva protokoly, aby si studenti uvědomili rozdíly mezi nimi a mohli posoudit vhodnost technologií pro různé situace. K laboratorním úlohám budou vypracovány návody, vzorová řešení a k práci budou přiloženy zdrojové soubory vytvořených programů v simulačním prostředí IT Guru.

# 1 PROSTŘEDÍ IT GURU

Programy od společnosti OPNET Technologies, Inc. slouží k návrhu, simulaci a analýze různých síťových mechanismů a technologií. Velkou předností simulačních programů je jejich grafické prostředí. Společnost OPNET dává na výběr ze dvou programů. Prvním z dvojice programů je OPNET Modeler v současné verzi 16.1 [11]. V tomto programu je možné simulovat chování více jak 800 síťových protokolů včetně IPv6, OSPFv3 a dalších. V OPNET Modeleru jsou také dostupné obsáhlé knihovny se zdrojovým kódem, který lze upravovat. Pro tuto práci, která se zabývá zejména základními síťovými protokoly, postačí druhá, základní verze IT Guru, která je ochuzena o několik funkcí a oproti verzi OPNET Modeler zaostává v podpoře síťových protokolů, ale nabízí jednu podstatnou výhodu pro studenty předmětu. Po zaregistrování na internetových stránkách společnosti je možné tuto verzi stáhnout a používat zdarma. Z těchto důvodů byla pro návrh laboratorních úloh zvolena tato základní verze, aby si studenti mohli laboratorní úlohy vyzkoušet i mimo školní učebnu.

## 1.1 Seznámení s prostředím IT Guru

Program IT Guru je simulační prostředí pro návrh, simulaci a analýzu síťových protokolů, mechanismů a technologií [10]. Velká výhoda tohoto simulačního prostředí spočívá v jeho grafickém prostředí, které umožňuje přehledně vytvářet síťový model. Další důležitou vlastností programu je velký výběr statistik, ze kterých můžeme vybírat jak globální statistiky pro celkový přehled sítě, tak statistiky pro jednotlivé síťové komponenty jako jsou například linky, síťové uzly, stanice a další. Program umožňuje simulovat chování sítě po dobu několika dní či týdnů v řádu minut či hodin. Simulovat lze též chování sítě v určitých situacích, které v reálném provozu ani nemusí nastat, například extrémní zatížení jednotlivých prvků.

## 1.2 Project editor

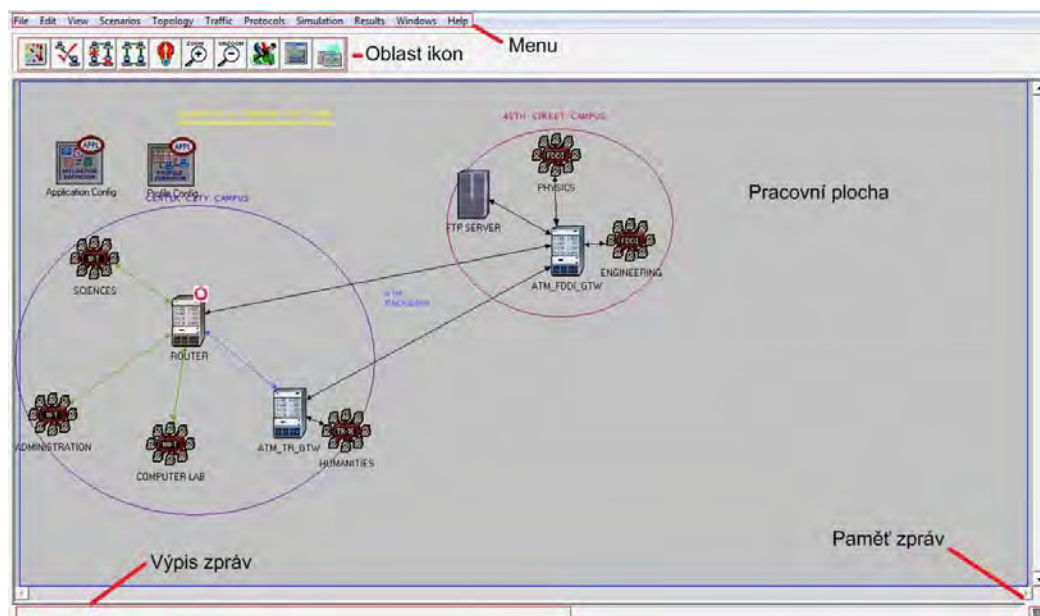
Project editor je hlavní část programu, v které se realizuje návrh topologie, vybírají

se požadované statistiky, zadávají se hodnoty pro simulaci a vlastní simulace se zde také spouští [10]. Project editor je rozdělen do několika logických částí, jak je znázorněno na obrázku 1.1. Na pozadí pracovní plochy project editoru lze při zakládání projektu vybrat libovolnou mapu, či zadat rozměry plochy v metrech, čehož se využívá například při práci s bezdrátovými sítěmi, aby bylo vidět, jak daleko od sebe jsou jednotlivé bezdrátové prvky umístěny.

V okně project editoru se nachází několik oblastí, které jsou důležité pro simulaci a sestavení síťového modelu:

- hlavní menu,
- oblast ikon,
- pracovní plocha,
- textová oblast,
- tipy.

Tyto části budou v dalších podkapitolách blíže popsány.



Obr. 1.1: Okno project editoru v prostředí IT Guru.

### 1.2.1 Hlavní menu

V hlavním menu lze podobně jako v jiných programech, přistupovat k jednotlivým

funkcím editoru. Hlavní menu je znázorněno na obrázku 1.2.



Obr. 1.2: Položky menu v IT Guru.

## 1.2.2 Oblast ikon



Obr. 1.3: Oblast ikon v project editoru prostředí IT Guru.

V této oblasti jsou zobrazeny nejdůležitější a nejčastěji používané funkce programu. Z obrázku 1.3 a tabulky 1.1 lze snadno vyčíst význam jednotlivých tlačítek.

Tab. 1.1: Popisky k funkcím ikon.

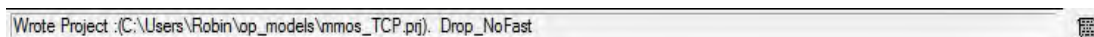
1	Otevře paletu objektů	6	Přiblížení pohledu
2	Zkontroluje konzistentnost linek	7	Oddálení pohledu
3	Vyřadí vybrané objekty	8	Konfigurace/spuštění simulace
4	Obnoví vybrané objekty	9	Zobrazí výsledky simulace
5	Přechod do nadřazené sítě	10	Zobrazí/schová všechny grafy

## 1.2.3 Pracovní plocha

Pracovní plocha je část project editoru, kam se umisťují jednotlivé komponenty z palety objektů pro vytvoření síťového modelu.

## 1.2.4 Textová oblast

Do textové oblasti se vypisují informace o stavu projektu (ukládání, změny a další). Ikona v pravé části textové oblasti (Obr. 1.4) se využívá ke zjištění posledních provedených operací (*message buffer*).



Obr. 1.4: Textová oblast programu IT Guru.

### 1.2.5 Tipy

Najetím kurzoru myši na ikonu nebo komponenty na pracovní ploše, se zobrazí okno s kontextovou nápovědou, ukázka je naznačena na Obr. 1.5.



Obr. 1.5: Zobrazení kontextové nápovědy.

## 2 TRANSPORTNÍ PROTOKOLY

UDP patří spolu s TCP mezi základní protokoly transportní vrstvy. Zprávám, které se pomocí protokolu UDP přenáší, říkáme datagramy. Protokol UDP poskytuje přenos datagramů bez záruky a kontroly doručení, jedná se o tzv. nespolehlivý a nespojovaný protokol [1]. Na rozdíl od TCP totiž nezaručuje, že se datagram po cestě neztratí, nedoručí se vícekrát, nebo že datagramy dorazí ve správném pořadí.

### 2.1 User Datagram Protocol (UDP)

Protokol UDP je pro svoje vlastnosti vhodný pro nasazení tam, kde se počítá se ztrátami datagramů a není vhodné, aby se nedoručené datagramy posílaly znovu, kvůli nežádoucímu zpoždění (IP telefonie, online hry,...). Při přenosu hlasových dat není až tak důležité, aby byl doručen úplně každý datagram, ale důležité je data přenést s co nejnižším a pokud možno konstantním zpožděním [3]. Vlastnosti UDP protokolu se také hodí pro systémy typu otázka-odpověď (např. *Domain Name System* - DNS).

Bitů 0 - 15	16 - 31
Zdrojový port	Cílový port
Délka dat	Kontrolní součet
Přenášená data	

Obr. 2.1: UDP datagram. [13]

Obrázek 2.1 znázorňuje strukturu UDP datagramu, význam jednotlivých polí je uveden dále v textu. Hlavička UDP datagramu obsahuje 4 pole.

**Zdrojový port** (*source port*) - 16 bitů, hodnota označuje číslo portu na straně odesílatele datagramu. Tato hodnota může být vynechána v případě, že odesílatel nepožaduje odpověď. Pokud se číslo zdrojového portu nepoužije, mělo by být pole nastaveno na hodnotu 0.

**Cílový port** (*destination port*) - 16 bitů, hodnota označuje číslo portu na straně příjemce datagramu.

**Délka dat** (*length*) - 16 bitů, udává délku UDP datagramu včetně přenášených dat. Hodnota je udávána v bajtech.

**Kontrolní součet** (checksum) – 16 bitů, kontrolní součet vytvořený jak z hlavičky, tak z dat. [1]

## 2.2 Transmission Control Protocol (TCP)

TCP protokol je jedním ze základních protokolů transportní vrstvy [1]. Tento protokol je, na rozdíl od UDP, spojově orientovaný a zaručuje spolehlivý (potvrzovaný) přenos dat. Protokol zaručuje, že se pakety doručí ve správném pořadí. Datové jednotce se při použití TCP protokolu říká segment. Protokol TCP před vlastním přenosem požadovaných dat, nejdříve navazuje spojení a případný ztracený paket během přenosu posílá znovu. TCP protokol je pro jeho spolehlivost nejvíce využívaným transportním protokolem. Služby, které využívají pro přenos TCP jsou například *File Transfer Protocol* (FTP), *Hyper Text Transfer Protocol* (HTTP), email, a další.

Bity 0 - 15							16 - 31						
Zdrojový port							Cílový port						
Pořadové číslo odesílaného bajtu													
Pořadové číslo potvrzovaného bajtu													
Délka záhlaví	Rezerva	U	A	P	P	S	F	Velikost okna					
		R	C	S	S	Y	I						
		G	K	H	T	N	N						
Kontrolní součet							Ukazatel naléhavých dat						
Volitelné a doplňující položky záhlaví													
Přenášená data													

Obr. 2.2: TCP segment. [15]

V následujícím textu je objasněn význam jednotlivých položek záhlaví.

**Zdrojový port** (*source port*) – 16 bitů, v poli uvedena hodnota zdrojového portu na straně odesílatele.

**Cílový port** (*destination port*) – 16 bitů, uvedená hodnota udává cílový port na straně příjemce.

**Pořadové číslo odesílaného bajtu** (*sequence number*) – 32 bitů, jednotlivé odesílané bajty se číslovají a pole obsahuje pořadové číslo prvního z odesílaných v TCP segmentu. Číslování nezačíná od nuly, ale od náhodně zvoleného čísla. Na začátku přenosu se generuje startovací pořadové číslo. ( ISN - initial sequence number)

**Pořadové číslo potvrzovaného bajtu** (*acknowledgment number*) – 32 bitů, vyjadřuje číslo následujícího bajtu, který je příjemce připraven přijmout. Jestliže příjemce naposledy přijal TCP segment s pořadovým číslem  $x$ , tak do tohoto pole ukládá číslo  $x + 1$ .

**Délka záhlaví** (*header length*) – 4 bity, délka záhlaví vyjadřuje délku záhlaví v násobcích 32 bitů (4 bajtů). Délka záhlaví může nabývat od 20 do 60 bajtů.

**Pole příznakových bitů** (*flags*) – 6 bitů, význam jejich nastavení na hodnotu 1 je:

- **URG** (*urgent*) – segment obsahuje naléhavá data,
- **ACK** (*acknowledgment*) – nastavení tohoto bitu udává, že daný segment slouží i jako potvrzovací,
- **PSH** (*push function*) – udává, že data mají být po přijetí předána aplikaci,
- **RST** (*reset the connection*) – používá se k odmítnutí spojení,
- **SYN** (*synchronize sequence number*) – pole využívané při navazování spojení,
- **FIN** (*no more data from sender*) – indikuje ukončení spojení,

**Délka okna** (*window size*) – 16 bitů, v poli uveden maximální počet bajtů, které je schopen přijímač přijmout bez potvrzení. (tzn., velikost vyhrazených paměťových prostředků pro dané spojení)



**Kontrolní součet** (*TCP checksum*) – 16 bitů, kontrolní součet je počítán nejen z položek TCP záhlaví, ale i z přenášených dat.

**Ukazatel naléhavých dat** (*urgent pointer*) – 16 bitů, pole využito pouze v případě nastavení příslušného příznakového bitu.

**Volitelné a doplňující položky záhlaví** (*options*) – pole může zůstat prázdné, jejich délku lze odvodit z celkové délky záhlaví uvedené v příslušné pozici, maximálně však 40 bajtů. [3],[1]

## 3 PŘENOSOVÉ TECHNOLOGIE

Kapitola zabývající se přenosovými technologiemi pojednává o dvou nejrozšířenějších technologiích v rámci LAN (*Local Area Network*), tedy o WLAN (*Wireless Local Area Network*) a Ethernetu. Jako síť LAN můžeme označit lokální síť, pokrývající malé geografické území, např. domácí, firemní nebo školní síť. Tyto sítě jsou spravovány buď samotnými uživateli (domácí sítě) nebo správci sítě (zaměstnanci dané společnosti). Přenosové rychlosti mohou být až v řádech Gbit/s.

### 3.1 Wireless Local Area Network (WLAN)

Pojem WLAN značí skupinu bezdrátových sítí, které jsou v poslední době hojně využívány zejména díky jednoduchosti instalace sítě a mobilitě klienta. Bezdrátové řešení má však i svá slabá místa, jako jsou náchylnost k rušení, vícecestné šíření signálu nebo například přístup ke sdílenému přenosovému kanálu. Bezdrátové sítě typu WLAN mají dosah v řádech desítek až stovek metrů, při použití směrových antén může být komunikační dosah v řádech kilometrů.

Bezdrátové sítě využívají k šíření dat prostorem elektromagnetických vln v rádiové, či optické oblasti spektra [9]. Nejznámější zástupce bezdrátových standardů na poli počítačových sítí je bezesporu standard IEEE 802.11 a jeho specifikace. Standard 802.11 bývá často označován svým obchodním jménem Wi-Fi. Standardy 802.11 využívají k přenosu bezlicenční radiová pásma ISM 2,4 a 5 GHz. Pro přístup ke sdílenému médiumu používají přístupovou metodu CSMA/CA (*Carrier Sense with Multiple Access and Collision Detection*), o které je pojednáno v následující kapitole.

#### 3.1.1 CSMA/CA

Přístupová metoda CSMA/CA je jedna z metod mnohonásobného přístupu na sdílené přenosové médium využívaná u sítí WLAN. Metoda spočívá v tom, že stanice, která chce vysílat „poslouchá“ provoz na kanálu. Když je kanál volný, stanice generuje náhodný časový interval, který určí jak dlouho má stanice ještě čekat, než může vysílat. Je-li kanál obsazený, stanice čeká, dokud se kanál neuvolní a opět čeká po dobu

časovače. Pokud po tuto dobu zůstane kanál volný, stanice začne vysílat.

U bezdrátových sítí s přístupovou metodou CSMA/CA může nastat problém „skrytého uzlu“ [9]. Stanice, která chce vysílat, „poslouchá“ kanál, ale může se stát, že mimo dosah této stanice, ale v dosahu přístupového bodu, vysílá jiná stanice. Tím dojde ke kolizi, kdy vysílají obě stanice. Protože stanice kolizi nemohou rozpoznat, vysílají data až do konce rámce, i když je to už zbytečné.

Tab. 3.1: Srovnání WLAN standardů.

	Rok schválení	Frekvence [GHz]	Rychlost [Mbit/s]	Modulace
802.11	1997	2,4	1 až 2	PSK
802.11a	1999	5	až 54	OFDM, PSK, QAM
802.11b	1999	2,4	až 11	PSK
802.11g	2003	2,4	až 54	shodné s 802.11a a 802.11b
802.11n	2007 (draft 2.0)	2,4 a 5	až 600	shodné s 802.11a a 802.11b

## 3.2 Ethernet

Technologie Ethernet je v současnosti nejvíce rozšířená přenosová technologie v sítích typu LAN. Prakticky všechny počítače v současnosti disponují síťovou kartou s Ethernetovým rozhraním RJ-45. Standard vyvinula firma Xerox v roce 1976. Původní přenosová rychlost byla 2,94 Mbit/s [1]. Nyní existuje mnoho verzí Ethernetu, které se liší zejména přenosovou rychlostí a použitým médiem (kroucená dvojlinka, koaxiální kabel, optické vlákno). Jednotlivé verze jsou standardizovány skupinou standardů 802.3. Základní přehled těchto standardů je ukázán v kapitole 3.2.2.

### 3.2.1 CSMA/CD

Pro přístup ke sdílenému médiu Ethernet využívá přístupové metody CSMA/CD (*Carrier Sense with Multiple Access and Collision Detection*) [9]. Metoda spočívá v tom, že stanice, která chce vysílat, nejprve po určitou dobu sleduje sdílené médium. Po zjištění volného kanálu začne ihned vysílat a současně kontroluje, jestli odeslaná data nenarušilo vysílání jiné stanice. V případě že stanice detekuje kolizi, vysílá

okamžitě signál JAM (zpráva dlouhá 32 bitů). Všechny stanice, které se kolize účastní, okamžitě přestanou vysílat. Každá stanice si pak vygeneruje náhodný časový interval, po který čeká, než opět zahájí vysílání. Tím, že vygenerovaný interval je náhodný, se eliminuje riziko, že dojde opět ke kolizi.

### 3.2.2 Verze Ethernetu

Během více než třicetiletého vývoje standardu vyšlo mnoho verzí a standardů Ethernetu, přehled poskytuje tabulka 3.2.

- a) **Ethernet** je prvním standardem s přenosovou rychlostí 10Mbit/s, Standard byl schválen v roce 1983.
- b) **Fast Ethernet** vychází ze standardního Ethernetu. Přenosová rychlost definována standardem IEEE 802.3u na 100Mbit/s. Zachovává shodnou architekturu i přístupovou metodu na medium jako u klasického Ethernetu.
- c) **Gigabitový Ethernet** navyšuje přenosovou rychlosti na 1 Gbit/s. První skupina standardů schválena v roce 1998. Původně byl definován pouze pro optická vlákna, ale byla doplněna i varianta pro kroucenou dvojlinku.
- d) **10 Gbit/s Ethernet** je v roce 2003 definován pro optická vlákna, později v roce 2008 dochází i ke standardizaci pro kroucenou dvojlinku. Standard zavádí plný duplexní provoz, tím odpadá potřeba metody CSMA/CD.
- e) **40/100 Gbit/s Ethernet** jsou standardy definované v roce 2010. Standardy jsou opět schváleny pro optická vlákna i metalické kabely. Metalické kabely mohou mít maximální délku 10 metrů. [1],[14]

Tab. 3.2: Přenosové rychlosti, standardy a verze Ethernetu. [9], [14]

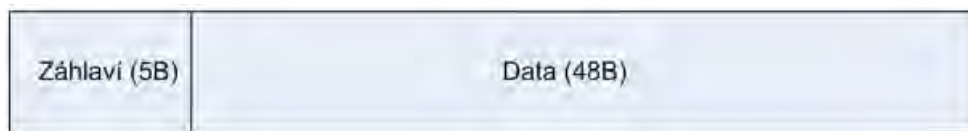
Rychlost sítě	Standard	Označení typů Ethernet
10 Mbit/s	IEEE 802.3	10Base-2, 10Base-5, 10Base-T, 10Base-FL, 10Base-FB, 10Base-FP, 10Broad-36
100 Mbit/s	IEEE 802.3u	100Base-TX, 100Base-T4, 100Base-FX
	IEEE 802.3xy	100Base-T2
1000 Mbit/s	IEEE 802.3z	1000Base-LX, 1000Base-SX, 1000Base-CX
	IEEE 802.3ab	1000Base-T
10 Gbit/s	IEEE 802.3ae	10GBase-SR, 10GBase-SW, 10GBase-LX4, 10GBase-LR, 10GBase-LW, 10GBase-ER, 10GBase-EW
	IEEE 802.3an	10GBase-T
40 Gbit/s	IEEE 802.3ba	40GBase-CR4, 40GBase-SR4, 40GBase-LR4, 40GBase-KR4
	IEEE 802.3bg	40GBase-FR
100 Gbit/s	IEEE 802.3ba	100GBase-CR10, 100GBase-SR10, 100GBase-LR4, 100GBase-ER4

## 4 PROTOKOLY PRO SÍŤ TYPU WIDE AREA NETWORK (WAN)

Sítě typu WAN (*Wide Area Network*) jsou rozsáhlé sítě s dosahem řádově stovky až tisíce kilometrů [9]. Jsou to sítě s nižší propustností často budované na pronajatých linkách, metodách přepínání okruhů nebo přepínání paketů. Používají se například pro propojení LAN sítí. V této práci se věnuje pozornost pouze protokolům ATM (*Asynchronous Transfer Mode*) a Frame Relay, tedy zástupci metody přepojování paketů respektive buněk.

### 4.1 Asynchronous Transfer Mode (ATM)

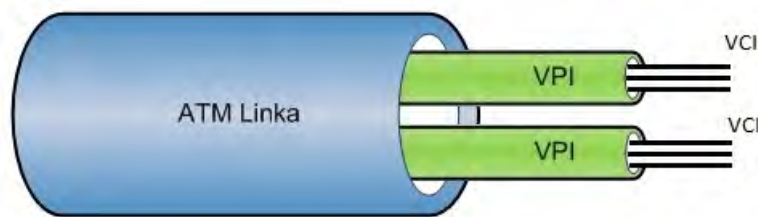
Technologie ATM vděčí za svůj vznik technologii *Broadband Integrated Services Digital Network* (B-ISDN), která potřebovala při vzniku přenosovou technologii pro přenos dat [12]. Nicméně později se z ATM stala univerzální přenosová technologie s pevně stanovenou délkou buňky 53 bajtů, z čehož je 5 bajtů záhlaví a 48 bajtů dat, viz obrázek 4.1. Velikost buňky 53 bajtů byla zvolena jako kompromis, tak aby byla technologie univerzální jak pro data, tak pro hlasové služby.



Obr. 4.1: ATM buňka.

#### 4.1.1 ATM síťová vrstva

Síťová vrstva ATM zajišťuje identifikace dat doručovaných od odesílatele k příjemci. U ATM se před vlastním přenosem ATM buněk musí sestavit virtuální spojení. ATM definuje dvě úrovně identifikátorů daného spoje [16]. Identifikátor virtuálního kanálu (VCI – *Virtual Channel Identifier*), což je identifikátor spoje mezi dvěma body a virtuální cestu (VPI – *Virtual Path Identifier*), která je svazkem několika VCI mezi dvěma uzly. Pro pochopení posloupnosti identifikátorů slouží obrázek 4.2.



Obr. 4.2: Identifikátory ATM spoje.

#### 4.1.2 ATM adaptační vrstva

Jelikož byla ATM technologie vyvíjena s ohledem jak na hlasové služby i pro data a každá z těchto aplikací má své specifické požadavky na přenosové parametry sítě definuje ATM třídy služeb [16]. Definované třídy služeb se označují buď písmeny A až D, nebo podle názvu pro jaký bitový tok jsou přizpůsobeny, viz následující rozdělení:

**CBR** (*Constant Bit Rate*) – třída využívaná pro konstantní bitovou rychlost, navržena pro služby, které jsou citlivé na kolísání přenosové rychlosti a zpoždění. Třída služeb CBR bývá taktéž označována písmenem A. Zejména se tedy jedná o služby přenosu hlasu, emulace digitálních okruhů a další. Při zahájení spojení jsou sjednány požadavky na přenosovou rychlost, ztrátovost a zpoždění a tyto parametry jsou rezervovány během celého spojení.

**VBR** (*Variable Bit Rate*) – pro variabilní přenosovou rychlost, označována taktéž písmenem B. Využíváno zejména pro přenos komprimovaného videa, kdy je přenosová rychlost závislá na změně a rychlosti obrázku. V této třídě služeb je tedy zajištěna proměnná přenosová rychlost, ale požadavky na zpoždění a kolísání zpoždění jsou podobné jako u CBR.

**ABR** (*Available Bit Rate*) – třída služeb ABR, neboli dostupná bitová rychlost, je využívána službami, které nejsou náchylné na zpoždění a kolísání zpoždění. Třída ABR může být označena písmenem C. Na rozdíl od předchozích dvou tříd služeb, třída služeb ABR nezajišťuje synchronizovaný přenos.

**UBR** (*Unspecified Bit Rate*) – může být označena písmenem D a shodně jako třída služeb ABR poskytuje nesynchronizované služby a navíc neposkytuje přenos se spojením. Při nasazení této vrstvy se aplikace musí spokojit s přenosovou kapacitou, která je právě k dispozici. Je-li tedy síť vytížená a nemá volné prostředky, může se stát,

že služby využívající této třídy služeb nebudou vůbec obslouženy.

Pro technologii ATM jsou v adaptační vrstvě specifikovány protokoly AAL-1 až AAL-5 (AAL – *ATM Adaptation Layer*). Služby třídy CBR používají protokol AAL-1, služby třídy VBR používají protokol AAL-2 a pro služby tříd ABR a UBR je využíván protokol AAL-5.

## 4.2 Frame Relay

Technologie Frame Relay představuje protokol pro WAN síť, který pracuje na fyzické a linkové vrstvě OSI modelu [1]. Frame Relay byl původně navržen také pro použití v sítích ISDN, ale později se z Frame Relay stala univerzální přenosová technologie. Formát Frame Relay rámce je znázorněn na obrázku 4.3, význam jednotlivých polí rámce je vysvětlen dále v textu.



Obr. 4.3: Formát rámce Frame Relay.

**Signalizace** – signalizační pole slouží k rozpoznání začátku a konce rámce, má vždy stejnou hodnotu 01111110 binárně.

**Adresa** – pole obsahuje 10ti bitové pole DLCI k identifikování virtuálního spoje a dále jednobitové značky BECN, FECN, DE, C/R a EA, které však pro tento text nejsou důležité a proto jim dále není věnována pozornost.

**Data** – pole obsahující uživatelská data nemá pevně stanovenou velikost. Pole může nabývat délky až 16000 bajtů.

**FCS (Frame Check Sequence)** – zabezpečení, kontrola rámce.

### 4.2.1 Typy síťových zařízení

Síťová zařízení mohou být u Frame Relay dvojího typu. Zařízení DTE (*Data Terminal Equipment*) a DCE (*Data Circuit-terminating Equipment*) [1]. Zařízení DTE představují koncová zařízení na straně zákazníka, jako jsou směrovače, mosty,



terminály a jiné. Naopak zařízení DCE přenáší data Frame Relay WAN sítí, většinou se jedná o Frame Relay přepínače.

#### **4.2.2 Virtuální okruhy**

Protokol Frame Relay poskytuje spojově orientovanou komunikaci, což znamená, že mezi dvěma koncovými terminály DTE musí být sestaveno spojení před vlastním přenosem dat. Protokol definuje použití permanentních (PVC – *Permanent Virtual Circuit*) i komutovaných virtuálních okruhů (SVC – *Switched Virtual Circuit*). V případě komutovaných spojů musí být před každým přenosem dat navázáno dočasné spojení mezi síťovými zařízeními [1]. PVC spoje jsou spoje permanentně nakonfigurované mezi síťovými zařízeními. Sestavený virtuální okruh mezi dvěma DTE zařízeními může procházet přes libovolný počet DCE zařízení Frame Relay WAN sítě. Každý virtuální okruh je identifikován číselnou adresou DLCI (*Data-link Connection Identifier*).

## 5 SMĚROVACÍ PROTOKOLY

Směrovací protokoly se dělí na IGP (*Interior Gateway routing Protocol*) a EGP (*Exterior Gateway routing Protocol*) [3]. Tato kapitola bude zaměřena na směrovací protokoly používané v rámci jednoho autonomního systému AS, tedy protokoly IGP.

Protokoly IGP se dále mohou dělit podle mechanismu, který používají k výběru nejvhodnější cesty sítí. V následujícím textu budou diskutovány dva hlavní zástupci IGP protokolů. Prvním z nich je RIP (*Routing Information Protocol*), což je zástupce skupiny *distance vector* směrovacích protokolů. Druhým diskutovaným směrovacím protokolem je OSPF (*Open Shortest Path First*), který se řadí do skupiny *link state*.

### 5.1 Routing Information Protocol (RIP)

Směrovací protokol RIP patří do podskupiny IGP protokolů typu *distance vector*. Protokoly typu *distance vector* jsou založeny na určování vzdálenosti a směrového vektoru do každé linky v síti [2]. Protokol RIP pro určení nejkratší cesty využívá tzv. Bellmanův-Fordův algoritmus, který je stručně popsán v následující kapitole. Jako metriku pro určení vzdálenosti do cíle využívá počet skoků (*hop count*). Pro zamezení vzniku smyček v síti je zvolen maximální počet skoků na 15. Směrovače si v pravidelných intervalech vyměňují celé směrovací tabulky, a to i v případě, že nenastala žádná změna v topologii sítě. V případě RIPu je tento interval 30 s. U sítí, kde se nepředpokládá častý zásah do topologie sítě, protokol RIP svojí režii zbytečně síť periodicky zatěžuje.

#### 5.1.1 Bellmanův-Fordův algoritmus

Bellmanův-Fordův algoritmus slouží pro nalezení nejkratších cest z jednoho uzlu do ostatních uzlů grafu s libovolným ohodnocením hran, tedy i záporným [4]. Při použití Bellmanova-Fordova algoritmu uzly neznají celou topologii grafu, jak je tomu u Dijkstrova algoritmu, viz kapitola 5.2.2. Základem Bellmanova-Fordova algoritmu je operace relaxace, do které vstupuje vždy cílový uzel, uzel od kterého přišla aktualizace a hrana mezi dvěma uzly. Pokud je hodnota uzlu, od kterého přišla aktualizace sečtená

s délkou hrany mezi uzly menší než aktuální hodnota nastavená na cílovém uzlu, cílový uzel si aktualizuje záznam o nejkratší cestě.

### 5.1.2 Verze protokolu RIP

- a) RIP – původní verze protokolu definována v RFC 1058 [2]. Pakety přenáší v pravidelných intervalech, nezahrnuje do nich masku sítě. Směrovací tabulky se šíří pomocí broadcast adresy.
- b) RIPv2 – náhrada první verze, řeší zejména její největší nedostatek, tedy nemožnost zasílat masky sítě v rámci aktualizací. Směrovače u této verze zasílají aktualizace na multicastové adrese 224.0.0.9. RIPv2 také umožňuje jednoduchou autentizaci.
- c) RIPv6 – (*RIP next generation*) standard definován v RFC 2080 zavádí podporu IPv6 adresace.

### 5.1.3 RIPv2 paket

Na obrázku 5.1 je znázorněn paket protokolu RIP verze 2 [5]. Dále v textu je vysvětlen význam jednotlivých polí paketu.

Bity 0 - 15		16 - 31
Command	Verze	Nepoužito (nastaveno na nuly)
AFI		Route tag
IP adresa		
Maska sítě		
Next hop		
Metrika		

Obr. 5.1: Paket RIPv2.

**Command** – znázorňuje, jestli se jedná o *žádost*, nebo *odezvu*. V případě *žádosti* směrovač požaduje zaslání celé nebo části směrovací tabulky. *Odezva* může být buď pravidelná nevyžádaná aktualizace, nebo odpověď na *žádost*.

**Verze** – specifikuje, která verze RIP protokolu je použita.

**Nepoužito** – nastaveno na nulu.

**AFI** (*Address Family Identifier*) – udává použité adresování uvnitř sítě. Protokol RIP je navržen univerzálně pro použití ve více protokolech. Pro IP adresaci je pole nastaveno na hodnotu 2. AFI ve verzi 2 také umožňuje jednoduchý autentizační mechanismus pro zabezpečení aktualizací směrovacích tabulek.

**Route tag** – znázorňuje metodu pro rozlišení mezi vnitřními záznamy naučenými RIP protokolem a záznamy naučenými z jiných směrovacích protokolů.

**IP adresa** – specifikuje IP adresu pro záznam.

**Maska sítě** – obsahuje masku sítě pro záznam. Jestliže je položka nastavena na nulu, tak pro daný záznam nebyla specifikována žádná maska.

**Next hop** – udává adresu, kam by pakety měly být posílány.

**Metrika** – udává počet směrovačů v cestě, neboli počet skoků. Tato položka může nabývat hodnot od 1 do 15 pro platnou cestu. Hodnota 16 znázorňuje nedosažitelný záznam.

## 5.2 Open Shortest Path First (OSPF)

Protokol OSPF patří do skupiny směrovacích protokolů typu *link state* a pro určení nejkratší cesty používá algoritmus *Shortest Path First* (SPF), který je založen na Dijkstrově algoritmu [1]. Tyto směrovací protokoly jsou charakteristické posíláním aktualizací směrovacích tabulek, jakmile nastane změna v topologii sítě.

Před vlastním zasíláním směrovacích informací musí jednotlivé směrovače nelézt své sousedy, k čemuž se používá tzv. „*Hello protokol*“. Při inicializaci nebo při změně ve směrovacích informacích směrovač vygeneruje „*Hello paket*“, ve kterém jsou uvedeny stavy linek ke všem připojeným směrovačům. Zprávy jsou u OSPF protokolu posílány záplavovým způsobem, což znamená, že jakmile směrovač obdrží „*Hello paket*“, uloží si ho a zprávu odešle všem svým sousedům [8]. Z důvodu optimalizování režijního provozu je u OSPF u *multiaccess* sítí (sítě s více jak dvěma směrovači) zvolen

*Designated Router* (DR) a *Backup Designated Router* (BDR). Směrovače pak nekomunikují přímo se svými sousedy, ale zprostředkovaně s DR, případně BDR, což je záložní směrovač, v případě výpadku DR. Nastane-li změna v topologii sítě, informace se nejdříve dostane k DR a poté je informace rozeslána od DR k jednotlivým podřízeným směrovačům v dané oblasti, viz kapitola 1.2.1. DR je zvolen na základě Router ID.

### 5.2.1 OSPF oblasti

V ustáleném stavu síťové topologie je zatížení sítě provozem OSPF poměrně malé. V případě, že často dochází ke změně topologie sítě, provoz krátkodobě naroste. Proto je v případě rozsáhlejších sítí vhodné rozdělit autonomní systém na jednotlivé oblasti (*areas*). Změna v topologii se promítne jen v aktualizacích směrovacích tabulek uvnitř dané oblasti a nezatěžuje se tak provozem celá síť. Oblasti jsou propojeny hraničními směrovači ABR (*Area Border Router*) [8]. Tyto směrovače znají topologii všech oblastí, které spojují. Oblasti jsou identifikovány 32 bitovým číslem.

Speciální úlohu má oblast s identifikátorem 0, které se říká tzv. páteřní oblast (*backbone area*). Všechny ostatní oblasti musí mít s touto oblastí hraniční směrovač ABR, tedy přímo s ní sousedit, nebo musí být propojeny virtuální linkou. Veškerý provoz směrovaný z jiné než páteřní oblasti (*inter area*) musí tedy procházet přes páteřní oblast 0, kromě případu kdy jde o provoz uvnitř dané oblasti (*intra area*).

### 5.2.2 Dijkstrův algoritmus

Dijkstrův algoritmus je nejrychlejší známý algoritmus pro nalezení všech nejkratších cest z jednoho uzlu do ostatních uzlů grafu, přičemž hrany musí nabývat pouze nezáporných hodnot [4]. Každý spoj dvou uzlů v síti (hrana) je ohodnocen určitou hodnotou, tzv. cenou. Tato cena je uvedena ve směrovacích tabulkách. Směrovače využívající protokol OSPF znají celou topologii sítě a proto na základě přiřazených cen mohou určit nejrychlejší cestu sítí.

### 5.2.3 Verze OSPF

V současnosti existují tři verze OSPF, které nejsou vzájemně zpětně kompatibilní.

První verze vznikla začátkem osmdesátých let a v roce 1991 byla nahrazena verzí OSPF 2 specifikované v RFC 1247 [7]. S blížícím se nástupem protokolu IPv6 nastala nutnost implementace nové verze OSPF, tedy verze 3. OSPF pro použití v IPv6 sítích byla definována v RFC 2740 v roce 1999.

#### 5.2.4 OSPF paket

Význam jednotlivých polí paketu OSPF protokolu (Obr. 5.2) je popsán v textu pod obrázkem. [8]

Bity 0 - 15		16 - 31
Verze	Typ	Délka paketu
ID směrovače		
ID oblasti		
Kontrolní součet		Typ autorizace
Autorizace		
Autorizace		

Obr. 5.2: OSPF paket.

**Verze** – znázorňuje použitou verzi OSPF.

**Typ** – znázorňuje typ OSPF paketu:

**Hello** – slouží pro navázání vztahů mezi sousedními směrovači.

**Database description** – tyto pakety se používají při zakládání vztahů mezi sousedními směrovači k výměně informací o obsahu směrovací tabulky.

**Link-state request** – požadavky na zaslání části směrovací tabulky od sousedních směrovačů.

**Link-state update** – odpověď na „*Link-state request*“ paket. Tyto pakety jsou také využívány při vytváření celé topologie sítě (flooding).

**Link-state acknowledgment** – potvrzení přijetí „*Link-state update*“ paketu.

**Délka paketu** – udává délku paketu v bytech včetně OSPF záhlaví.

**Router ID** – znázorňuje zdroj paketu.

**Area ID** – udává oblast, do které paket patří.

**Kontrolní součet** – slouží ke kontrole, jestli nedošlo ke změně obsahu dat během přenosu.

**Typ autorizace** – obsahuje typ ověření. Všechny výměny paketů v rámci OSPF protokolu jsou ověřovány.

**Autorizace** – obsahuje ověřovací informace.

### 5.3 Shrnutí ke směrovacím protokolům

Z předešlého textu je patrné, že směrovací protokol RIP je vhodný využívat zejména v jeho druhé verzi, v které přenáší informace o maskách sítě a může tak být využito beztřídní adresování. Protokol RIP je nevhodné využívat na spojích, kde nedochází k častým změnám v síti. RIP protokol zbytečně zatěžuje síť svým provozem. Protokol OSPF je oproti RIP protokolu náročnější na přenosovou kapacitu sítě při budování směrovacích tabulek. Při udržování směrovacích tabulek, kde nedochází ke změnám v topologii sítě protokol OSPF zatěžuje síť pouze minimálně. Protokol OSPF je ovšem náročnější na výpočetní výkon směrovačů při budování směrovacích tabulek a výpočtu SPF algoritmu.

## 6 LABORATORNÍ ÚLOHY

V rámci diplomové práce je vytvořen návrh 4 laboratorních úloh pro prostředí IT Guru. K laboratorním úlohám byl vytvořen podrobný návod pro studenty včetně doplňujících otázek a úkolů a programů v simulačním prostředí. Dále bylo zpracováno pro každou úlohu vzorové řešení.

Jednotlivé návody k laboratorním úlohám obsahují stručný úvod k dané úloze. Úlohy jsou členěny do několika logických celků (úkolů), přičemž na konci každého celku je série doplňujících otázek či úkolů. Odpovědi na tyto otázky respektive vypracování daného úkolu by si studenti měli zaznamenat tak, aby výsledky na konci laboratorního cvičení mohli prezentovat cvičícímu.

Při vytváření laboratorních úloh byl kladen důraz na co nejpodrobnější popsání postupu vytvoření programu. Samostatná práce studentů se předpokládá při realizaci doplňujících otázek a úkolů. Laboratorní úlohy a zejména pak doplňující otázky a úkoly by měly studentům pomoci s pochopením a procvičením dané problematiky.

První vytvořená úloha v rámci této práce je zaměřena na srovnání dvou transportních protokolů TCP a UDP. Při vytváření této úlohy byl kladen důraz na to, aby si studenti při realizaci úlohy uvědomovali rozdíly mezi těmito protokoly a vhodnost použití pro různé aplikační protokoly.

Další úloha srovnává fyzické přenosové technologie WLAN a Ethernet. Návrh této úlohy byl limitován omezeností bezplatné verze IT Guru. V programu je implementována maximální přenosová rychlost pro bezdrátové přenosy na 11 Mbit/s. Proto byla v úloze u klientské části ethernetové topologie využita technologie 10BaseT, aby teoretické maximální přenosové rychlosti byly srovnatelné. Úloha je zaměřena na porovnání přenosových parametrů jednotlivých technologií pro různé vytížení sítě a také na vliv vzdalování bezdrátového klienta od přístupového bodu.

V úloze srovnávající směrovací protokoly byly pro návrh úlohy vybrány směrovací protokoly RIP a OSPF, tak aby se studenti seznámili s rozdíly mezi dvěma základními skupinami směrovacích protokolů IGP, a to *link state* a *distance vector*. V úloze se studenti seznámí s rozdíly v distribuci směrovacích tabulek, rychlosti konvergence a rozdíly ve směrovacích tabulkách směrovacích protokolů OSPF a RIP ve verzích



RIPv1 a RIPv2.

Poslední navrhnutá úloha je zaměřena na technologie pro sítě typu WAN. V rámci této úlohy se studenti seznámí s konfigurací ATM technologie a třídění provozu do jednotlivých tříd služeb A až D definovaných pro ATM. Druhá část úlohy je zaměřena na technologii Frame Relay a konfiguraci virtuálních okruhů mezi dvěma směrovači. V úloze je u technologie Frame Relay ukázáno třídění provozu do jednotlivých tříd služeb ToS (*Type of Service*).

V návodech laboratorních úloh pro studenty a vzorovém řešení úloh jsou použity výstupy přímo z programu IT Guru. Přestože výstupy mají určité typografické nedostatky, byly použity z důvodu názornosti pro studenty. Studenti si tak mohou přímo ověřit, jestli konfigurovali vše správně a jestli se dopravovali ke správným výsledkům.

## 7 SROVNÁNÍ PROTOKOLŮ TCP A UDP

### 7.1 Úvod k laboratorní úloze

Tato úloha je zaměřena na srovnání dvou základních protokolů transportní vrstvy. Zatímco UDP je velmi jednoduchý protokol a poskytuje nespolehlivou (nepotvrzovanou) službu, protokol TCP se označuje jako spolehlivý a snaží se o doručení každého paketu.

### 7.2 Úkol 1 – vytvoření topologie

V prvním úkolu této úlohy vytvoříte základní topologii a provedete nastavení jednotlivých komponent. K vytvoření provozu nebudete používat přednastavené aplikace, ale definujete si vlastní síťový provoz pomocí komponenty *Task*. Vytvoříte dva scénáře. Jeden scénář nakonfigurujete tak, aby pro přenos využíval protokol TCP, druhý scénář bude používat protokol UDP.

#### 7.2.1 Popis vytvoření programu

1. Spusťte program OPNET IT Guru Academic Edition.
2. Z menu programu vyberte položku **File/New...** (Ctrl + N) a v rolovací nabídce ponechejte „Project“ a potvrďte tlačítkem **OK**.
3. V následujícím okně zadejte jméno projektu a scénáře. Jméno projektu zvolte například „*Srovnani\_TCP\_UDP*“ (*Project Name*) a jméno scénáře „TCP“ (*Scenario Name*).
4. Následně nechte vybranou položku „Create Empty Scenario“ a klikněte na **Next**.
5. Při výběru rozlohy označte položku „Campus“ a ponechejte zaškrtnuté „Use Metric Units“ a klikněte na **Next**.
6. Nyní zadáváte požadovanou rozlohu, kterou ponechejte na výchozích hodnotách, tedy 10x10 km.
7. V následujícím kroku máte na výběr několik technologií. Zatrhněte „ethernet\_advanced“, „internet toolbox“, „routers“ a klikněte na **Next**. Poté potvrďte

volbou **OK** požadované nastavení, které si ještě jednou můžete zkontrolovat v přehledu.<sup>12</sup>

8. Vložte na plochu postupně tyto komponenty z okna *Object Palette*:
  - I. Application Config
  - II. Profile Config
  - III. Task Config
  - IV. ip32\_cloud
  - V. 2x subnet
9. Komponenty rozmístěte na plochu a pojmenujte podle obrázku 7.1. Přejmenování prvku provedete kliknutím pravým tlačítkem myši na daný prvek a z kontextového menu vyberete možnost *Set Name*.



Obr. 7.1: Základní topologie úlohy.

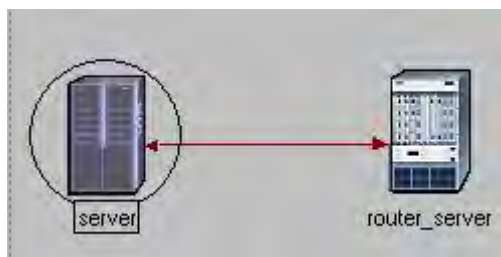
10. Dvojitým kliknutím na ikonu podsítě serveru (subnet\_server) vstupte do podsítě a z okna *Object Palette* vložte server „ethernet\_server\_adv“ a směrovač „ethernet2\_slip8\_gtwy“. Komponenty pojmenujte podle obrázku 7.2. Server

<sup>1</sup> Stejně jako při práci s jakýmkoliv jiným programem doporučuji práci průběžně ukládat (Ctrl + S). Při prvním uložení se program IT Guru dotáže, jestli opravdu chcete uložit projekt pod již definovaným názvem při zakládání projektu. Uložení je vhodné provádět vždy po změně či nastavení nějaké z komponent, tak aby se nastavené parametry zpřístupnili i pro nastavování dalších komponent.

<sup>2</sup> Ve vytvořeném projektu můžete tlačítky  a  přiblížit či oddálit požadovanou oblast.

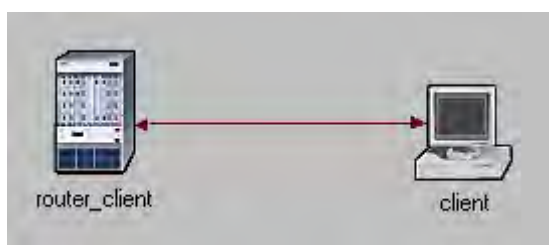
a směrovač propojte technologií Ethernet 10BaseT<sup>3</sup> přetažením ikony 10BaseT z okna *Object Palette* na pracovní plochu a prostým spojením obou komponent.

V dalším kroku nastavte adresu serveru na hodnotu „server“. Nastavení provedete tak, že pravým tlačítkem kliknete na objekt „server“, vyberete *Edit Attributes* a do položky *Server Address* napíšete „server“.



Obr. 7.2: Podsíť serveru.

11. V dalším kroku proveďte obdobnou konfiguraci pro klientskou podsíť (subnet\_client).<sup>4</sup> Místo serveru však vložte objekt „ethernet\_wkstn\_adv“. Opět pojmenujte komponenty (Obr. 7.3) a adresu klienta nastavte na hodnotu „client“.




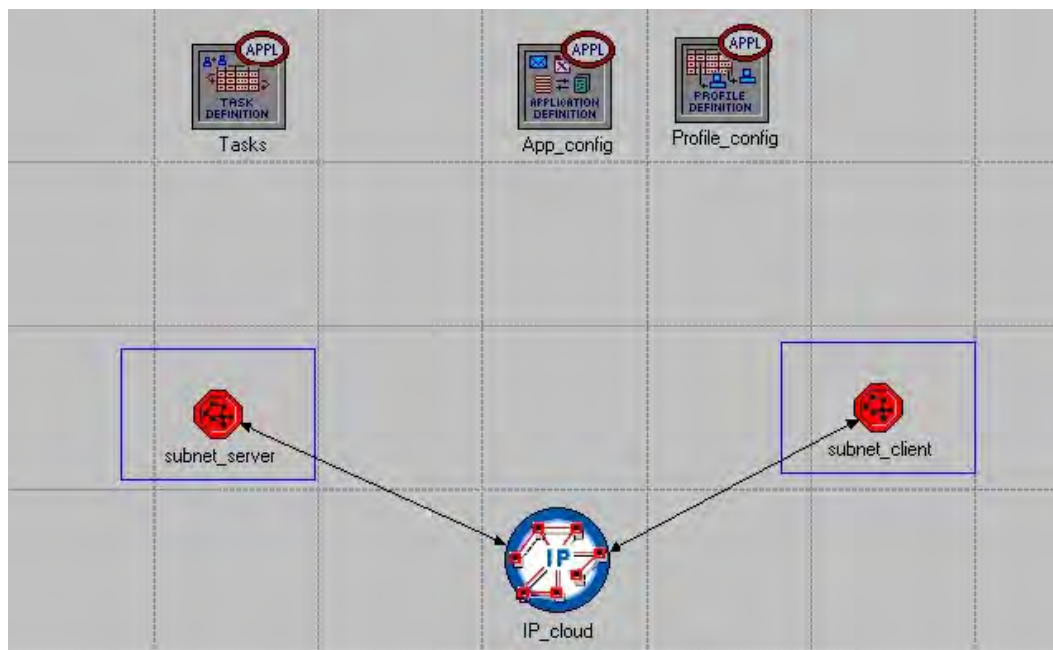
Obr. 7.3: Klientská podsíť.

12. Pro dokončení základní topologie ještě zbývá propojit oba směrovače s komponentou „IP\_cloud“. Propojení proveďte technologií „PPP\_DS3“.

---

<sup>3</sup> Pro propojení uvnitř klientské podsítě budete využívat technologii 10BaseT, na rozdíl od zbylé části sítě, kde budete prvky sítě spojovat technologií 100BaseT. Vysvětlení je uvedeno dále v textu.

<sup>4</sup> pro přechod z podsítě do nadřazené sítě můžete použít tlačítko , nebo klikněte na plochu pravým tlačítkem a z kontextového menu vyberte možnost „Go To Parent Subnet“.

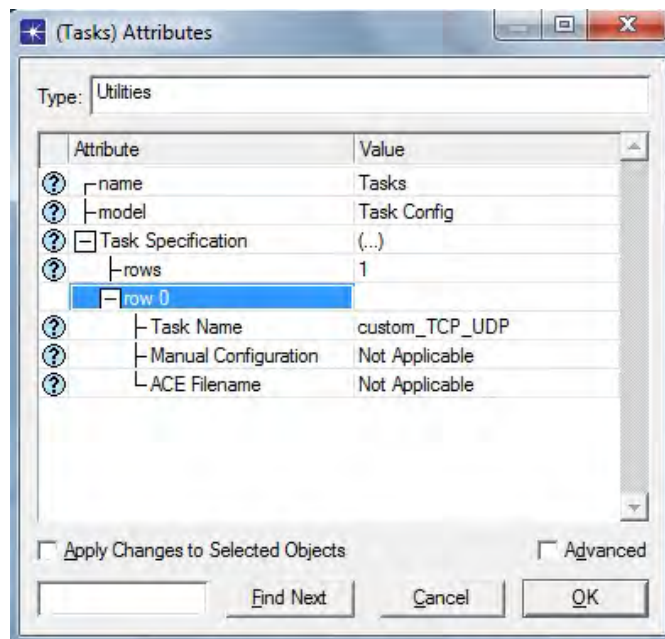


Obr. 7.4: Propojení IP\_cloud a směrovačů technologií DS3.

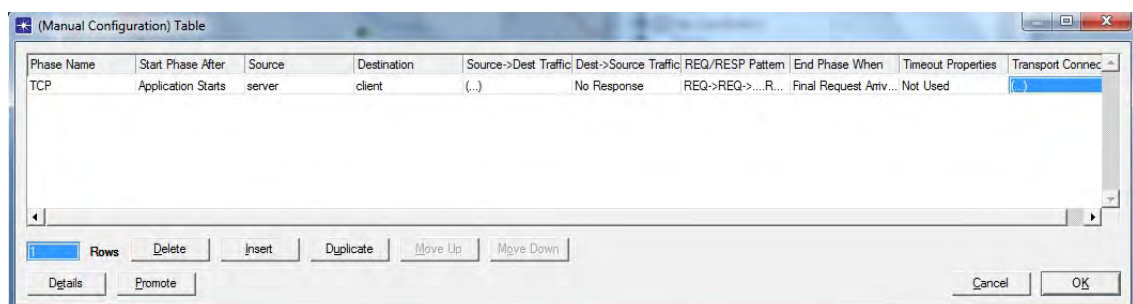
Propojení objektu uvnitř podsítě s objektem vně podsítě provedete v nadřazené síti propojením dané podsítě s požadovaným objektem. Po propojení se program zeptá, se kterým objektem uvnitř podsítě chcete spojit, a nabídne možnosti, z kterých vyberete vámi požadovaný objekt. V našem případě budete tedy propojovat objekty **IP\_cloud** s **subnet\_server** a **IP\_cloud** s **subnet\_client** a při dotazu programu zvolíte možnost `subnet_server.router_server` a `subnet_client.router_client` pro zvolení směrovače uvnitř jednotlivých podsítí.

13. Nyní máte vytvořenou základní topologii a postoupíte k nastavení jednotlivých komponent. Začněte s komponentou *Tasks*, pomocí které budete generovat vlastní síťový provoz. Vstupte známým způsobem do nastavování atributů komponenty *Tasks* (pravým tlačítkem kliknete na komponentu a vyberete *Edit Attributes*).

V položce *Task Specification* nastavte *Rows* na 1 a do položky *Task Name* napište jméno, např. „custom\_TCP\_UDP“ (Obr. 7.5). V dalším kroku vyberte *Manual Configuration* a zvolte *Edit...* V novém okně opět změňte počet *Rows* na 1 a nastavte podle obrázku 7.6.

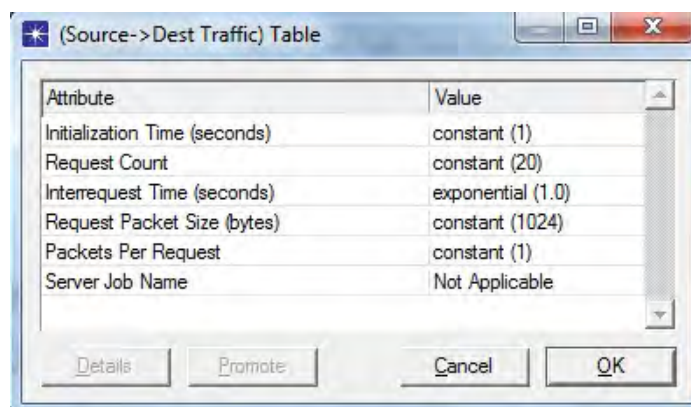


Obr. 7.5: Nastavení komponenty Task.



Obr. 7.6: Nastavení vlastní aplikace v *Manual Configuration*.

V položce *Source -> Dest Traffic* nastavujete vlastní síťový provoz. Parametry nastavte podle obrázku 7.7.



Obr. 7.7: Definice síťového provozu.

Poslední položka, kterou budete v *Manual Configuration* nastavovat je *Transport Connection*, kde nastavte:

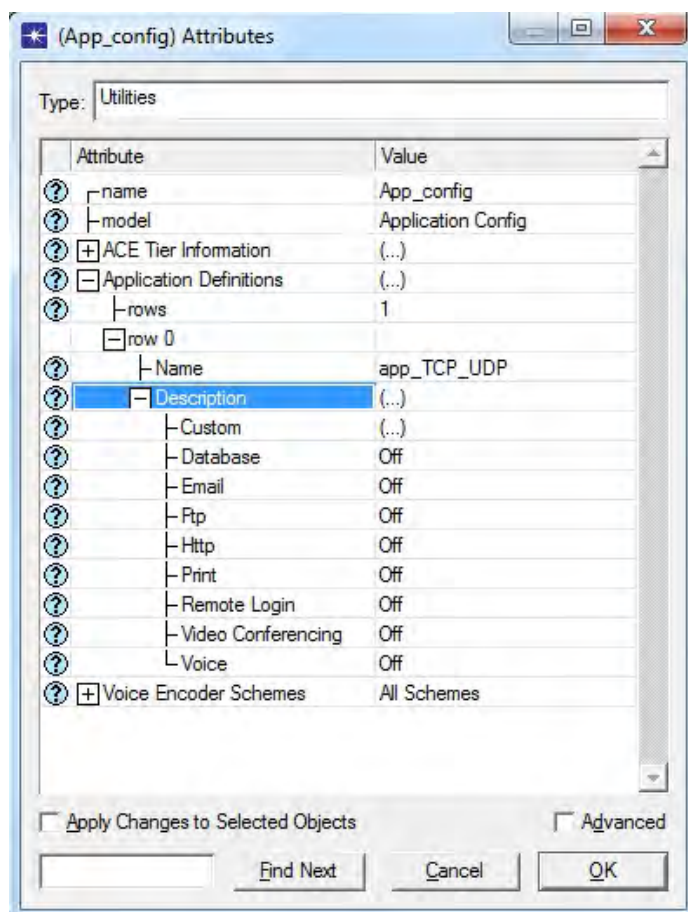
*Policy* na „Reuse Connection“,

*Limit* na „Unlimited“ a

*Transport Protocol* na „TCP“.

Nastavení potvrďte a uložte tlačítkem OK.

14. Nyní budete nastavovat komponentu *App\_config*, čehož opět docílíte kliknutím pravého tlačítka myši na komponentu a vyberete *Edit Attributes*. V záložce *Application Definitions* nastavte *Rows* na 1 napište jméno aplikace „app\_TCP\_UDP“, viz Obr. 7.8.

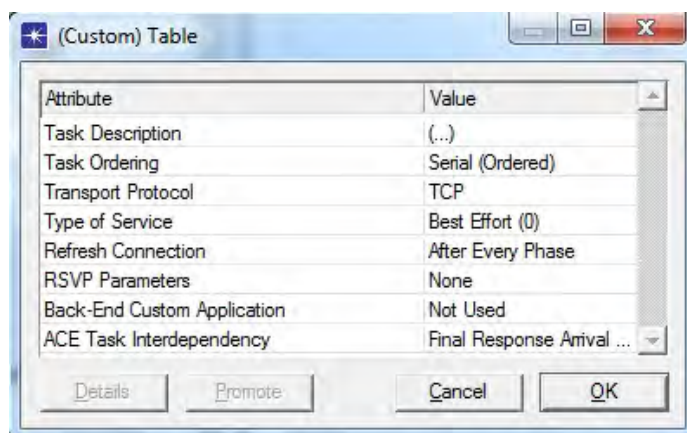


Obr. 7.8: Definice aplikace v okně *Application Config*.

Dále přistupte k vlastnímu nastavení aplikace. Protože v úloze budete

porovnávat dva transportní protokoly a každý z definovaných protokolů je vázán vždy k jednomu z nich, použijete vlastní (Custom) aplikaci, pro kterou jste si již definovali provoz v komponentě *Tasks*.

Nastavení proved'te kliknutím na *Custom* a výběrem *Edit...* Další nastavení proved'te podle obrázku 7.9.

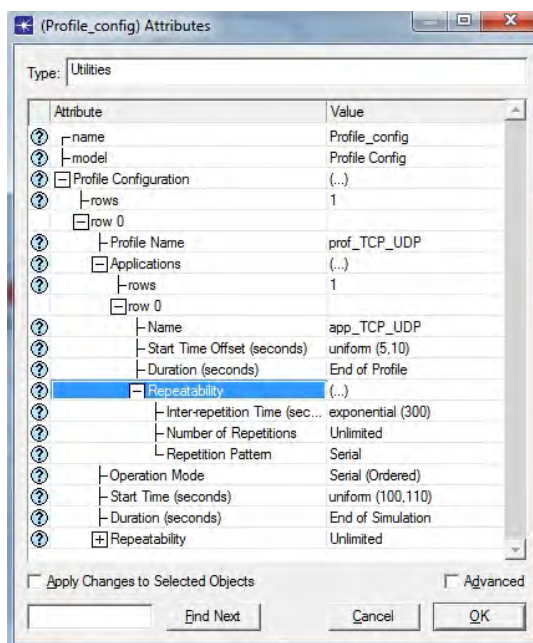


Obr. 7.9: Nastavení vlastní (*custom*) aplikace.

V položce *Task Description* opět zvolte *Edit...*, počet *Rows* nastavte na 1 v poli *Task Name* vyberte již připravený Task pojmenovaný „custom\_TCP\_UDP“. Všechno nastavení potvrďte tlačítkem *OK* a projekt uložte.

15. Komponentu *Profile\_config* nastavte podle obrázku 7.10. Definujte si jméno profilu „prof\_TCP\_UDP“ a v poli *Applications* změňte počet *Rows* na 1 a vyberte vytvořenou aplikaci „app\_TCP\_UDP“. Dále poslední možnou položku *Repeatability* pro vytvořený profil nastavte na „Unlimited“. Výběr a nastavení potvrďte tlačítkem *OK* a projekt opět uložte.





Obr. 7.10: Nastavení parametrů profilu pro aplikaci.

16. Po nastavení aplikace a profilu musíte ještě zajistit podporu této aplikace a profilu na serveru a klientovi. Proto vstupte do konfigurace atributů (*Edit Attributes*) na **serveru**. Z nabídky nejprve vyberte *Application: Destination Preferences* a klikněte na *Edit...* Změňte počet Rows na 1 a v poli *Symbolic Name* vyberte „client“. Dále klikněte na pole *Actual Name*, změňte počet Rows na 1 a opět vyberte „client“. Nastavení potvrďte až k nastavení parametrů serveru, kde budete nastavovat ještě další položky.

V poli *Application: Source Preferences* klikněte na *Edit...* a v poli *Symbolic Name* vyberte „server“. Dále v nastavení serveru v poli *Application: Supported Profiles* vyberte dříve definovaný profil „prof\_TCP\_UDP“. V poli *Application: Supported Services* vyberte dříve definovanou aplikaci „app\_TCP\_UDP“. Nastavení serveru potvrďte a projekt uložte.<sup>5</sup>

17. Nastavení **klienta** bude probíhat obdobně. V poli *Application: Destination Preferences* v poli *Symbolic Name* vyberte „client“ a dále v poli *Actual Name* hodnotu „client“. Položku *Application: Source Preferences* **nenastavujte**. V poli

<sup>5</sup> Pokud se vám nezpřístupní některá nastavení v rámci jedné komponenty, např. výběr podporovaného profilu, provedená nastavení potvrďte a ukončete editaci komponenty. Uložte projekt (Ctrl+S) a vstupte znovu do editace atributů komponenty.

*Application: Supported Profiles* nastavte opět dříve vytvořený profil „prof\_TCP\_UDP“. Pole *Application: Supported Services* na klientovi **nenastavujte**.

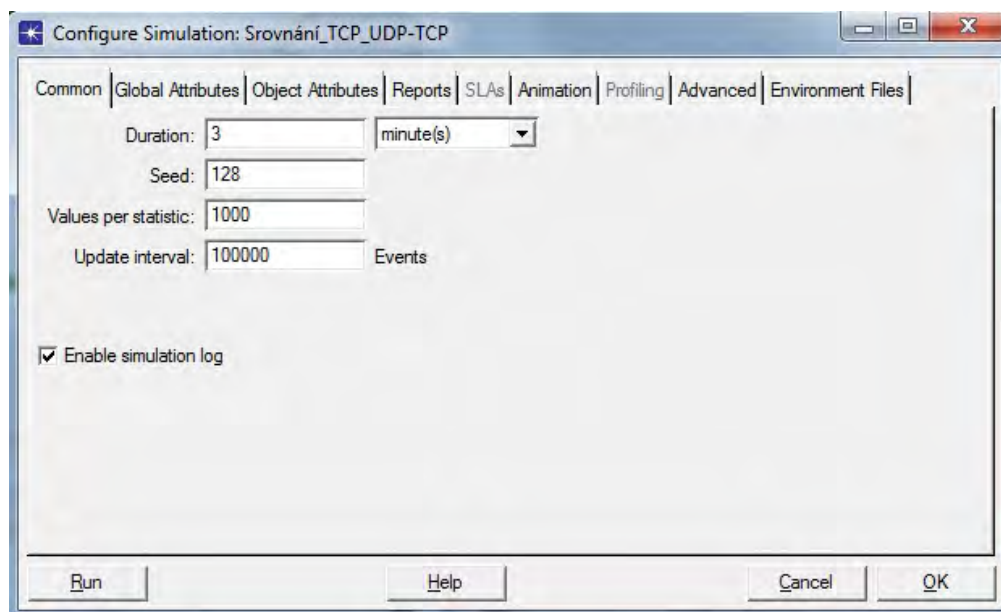
18. Po nakonfigurování základní topologie a jednotlivých komponent přistupte k vybrání statistik, které budete sledovat. Statistiku vyberete kliknutím pravého tlačítka myši na plochu a z nabídky vyberete *Choose Individual Statistics*. Z nabízených statistik vyberte následující:

- a) Global Statistics: Custom Application/Traffic Received (bytes/sec)  
Custom Application/Traffic Sent (bytes/sec)  
Custom Application/Traffic Received (packets/sec)  
Custom Application/Traffic Sent (packets/sec)
- b) Node Statistics: IP/Traffic Received (packets/sec)  
IP/Traffic Sent (packets/sec)  
TCP/Traffic Received (bytes/sec)  
TCP/Traffic Received (packets/sec)  
UDP/Traffic Received (bytes/sec)  
UDP/Traffic Received (packets/sec)
- c) Link Statistics: point-to-point/queuing delay -->  
point-to-point/queuing delay <--  
point-to-point/throughput (bits/sec) -->  
point-to-point/throughput (bits/sec) <--

19. Po vybrání sledovaných statistik můžete přistoupit k vlastní simulaci. Stisknutím



ikony (Run) se dostanete do konfiguračního okna simulace, kde nastavte čas simulace na 3 minuty, počet hodnot na statistiku 1000 a obnovovací interval na 100000 hodnot. (Obr. 7.11) Po nastavení požadovaných parametrů stiskněte tlačítko **Run** pro zahájení simulace.

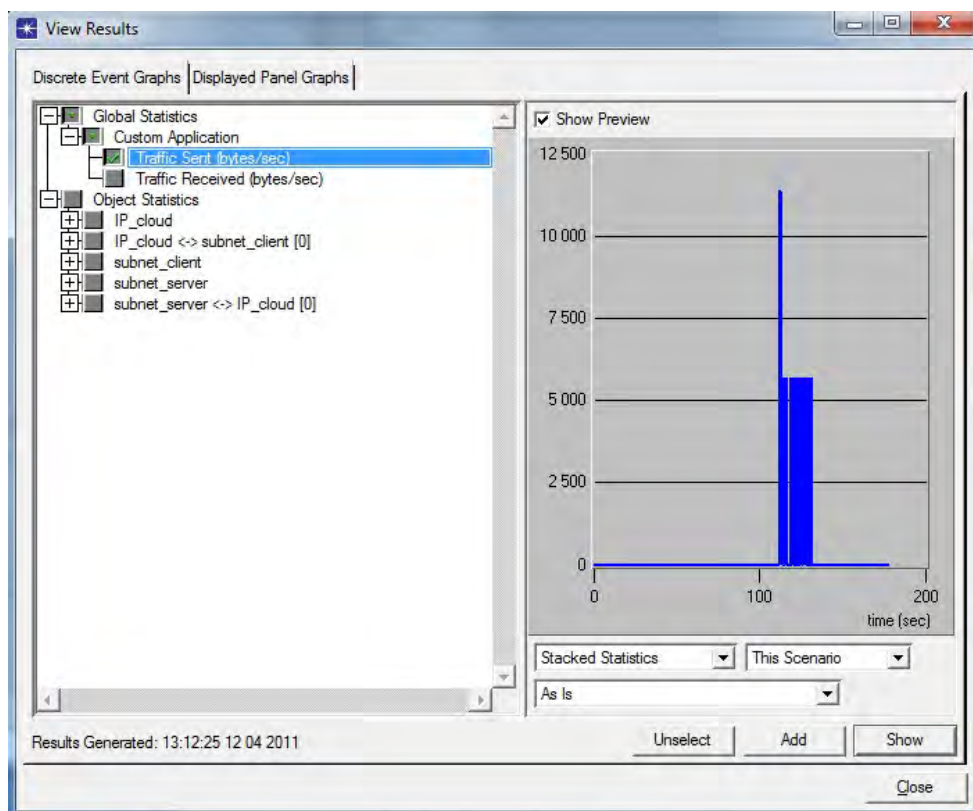


Obr. 7.11: Nastavení parametrů simulace.

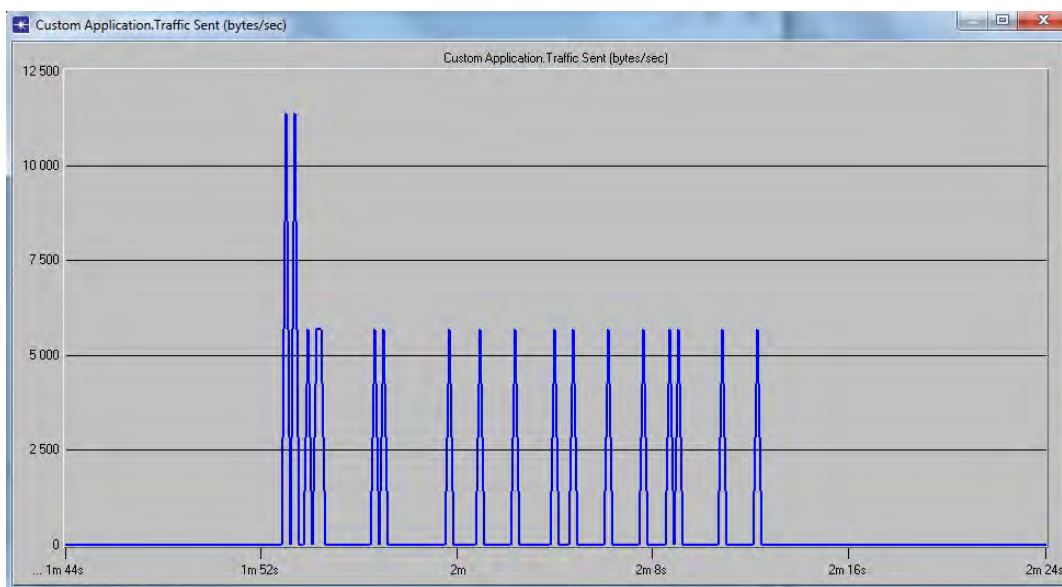
20. Pro zobrazení výsledků klikněte pravým tlačítkem myši na plochu a z nabídky vyberte *View Results*.<sup>6</sup> Po vybrání grafu z *Global Statistics/Custom Application* a zaškrtnutí políčka *Traffic Sent (bytes/sec)* byste měli vidět graf shodný s obrázkem 7.12.

---

<sup>6</sup> Graf lze zobrazit po zmáčknutí tlačítka **Show** a v grafu pomocí kurzoru myši vybrat požadovanou oblast pro přiblížení, podobně jak tomu je na obrázku 7.13. Pro navrácení zobrazení celého grafu můžete využít pravé tlačítko myši a vybrat „Full Horizontal Scale“ a „Full Vertical Scale“.



Obr. 7.12: Ukázka okna výsledků.

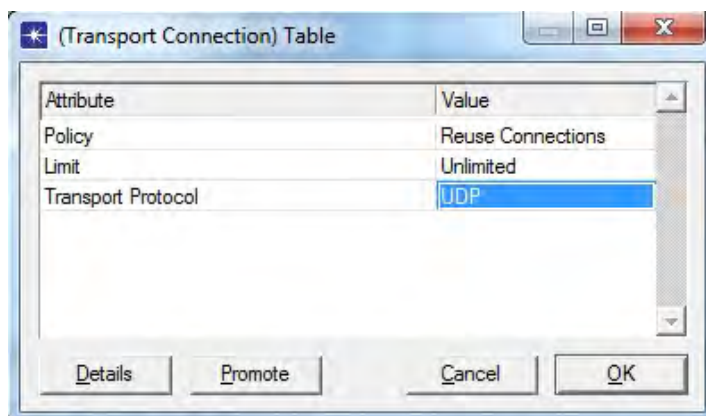


Obr. 7.13: Detail statistiky pro vlastní aplikaci v bajtech/s.

21. Po úspěšném zobrazení grafu a ověření správnosti nakonfigurování jednotlivých prvků rozšířte projekt o další scénář. K vytvoření nového scénáře využijte možnost duplikování současného scénáře. Toho docílíte vybráním položky menu

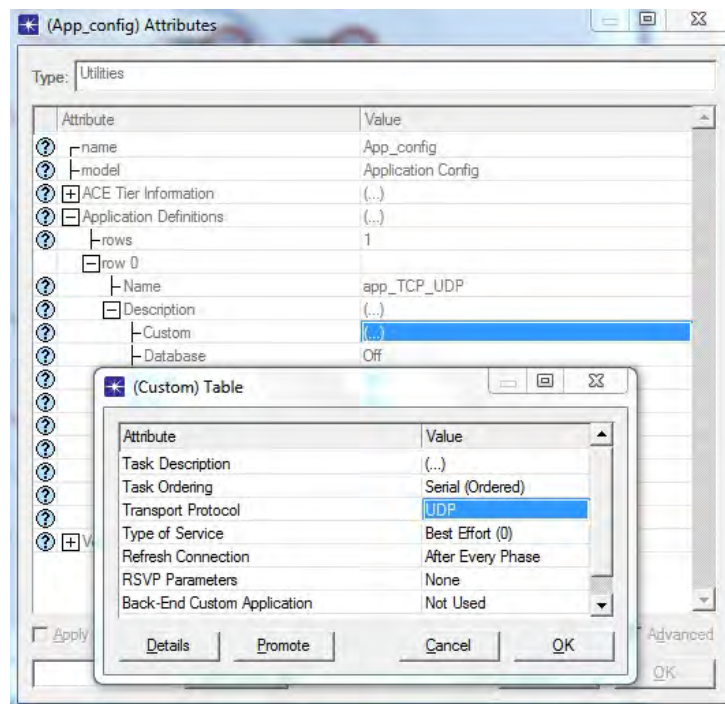
*Scenarios/Duplicate Scenario* a zadáním jména nového scénáře. Nový scénář pojmenujte „UDP“.

22. Nový scénář UDP upravte tak, aby k přenosu dat využíval transportní protokol UDP místo TCP. První z komponent, kterou upravíte je komponenta *Tasks*, kde vstoupíte do konfigurace a v položce *Task Specification* dáte editaci položky *Manual Configuration*. V tomto okně změníte hodnotu *Phase Name* na „UDP“ a v poli *Transport Connection* zvolíte *Transport Protocol* „UDP“. (Obr. 7.14)



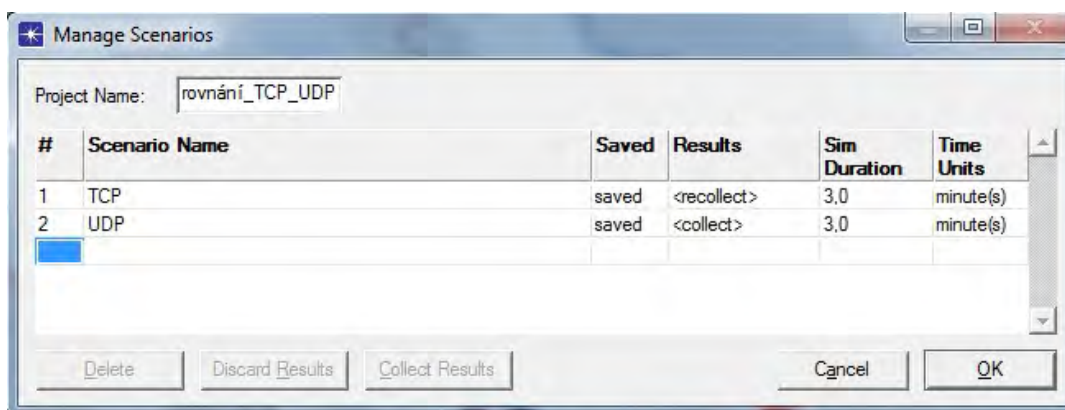
Obr. 7.14: Nastavení UDP protokolu pro aplikaci.

Druhou změnu v novém scénáři provedete v nastavení komponenty *Application Config*, kde uvnitř vámi definované aplikace dáte editaci *Custom* protokolu a opět zvolíte *Transport Protocol* „UDP“. (Obr. 7.15)



Obr. 7.15: Nastavení UDP protokolu ve vlastní (*custom*) aplikaci.

23. Po nakonfigurování druhého scénáře je nutné znovu simulovat chování sítě. K tomu nyní nevyužívejte tlačítko Run jako v předchozím případě, ale vyberte z nabídky *Scenarios/Manage Scenarios...* a u položek *Results* vyberte *<collect>* respective *<recollect>*. Délku simulace ponechte na 3 minuty a potvrďte volbu tlačítkem **OK**.



Obr. 7.16: Nastavení parametrů v *Manage Scenarios*.

## 7.2.2 Doplnující otázky a úkoly<sup>7</sup>

- 1) Zobrazte si výsledky simulace a jednotlivé statistiky si projděte.

<sup>7</sup> Odpovědi na otázky si poznamenejte a na konci cvičení je přednesete vyučujícímu.



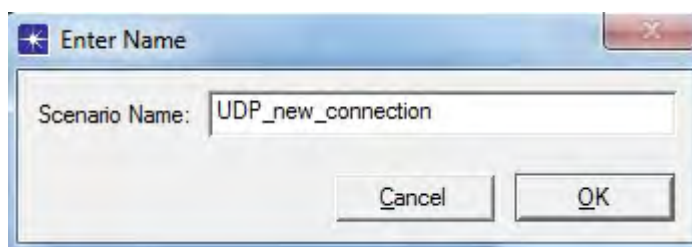
- 2) Zobrazte si statistiku *Global Statistics/Custom Application/Traffic Sent* pro oba scénáře. Zobrazené grafy porovnejte a zdůvodněte, proč jsou grafy rozdílné. Zaměřte se zejména na rozdíl v délce trvání jednotlivých statistik.
- 3) To, že ve statistikách „TCP“ a „UDP“ jednotlivých prvků (Object Statistics) můžete pozorovat data vždy pro konkrétní protokol je logické. Zamyslete se ale nad tím, jak je možné, že ve statistikách „IP“ můžete pozorovat data z obou scénářů. Vysvětlíte posloupnost zapouzdřování dat.
- 4) Vyjmenujte alespoň 2 aplikační protokoly, které používají transportní protokol UDP a 3, jenž využívají protokol TCP.
- 5) Zdůvodněte, proč např. protokol FTP používá protokol TCP a VoIP protokol UDP?

## 7.3 Úkol 2 – navazování spojení

V tomto doplňujícím úkolu budete konfigurovat nové scénáře, ve kterých nastavíte aplikace tak, aby se při každém přenosu navazovalo nové spojení.

### 7.3.1 Postup

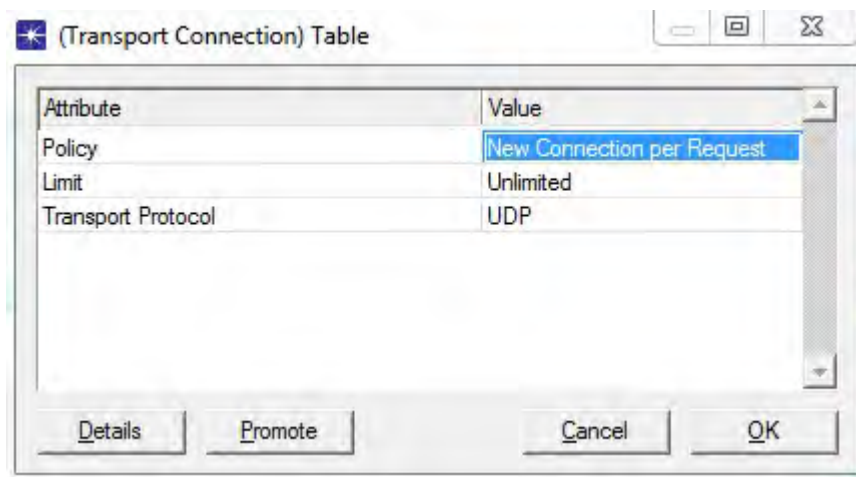
1. Duplikujte oba vytvořené scénáře (*Scenarios/Duplicate Scenario*). Pro přepínání mezi jednotlivými scénáři lze využít položku menu *Scenarios/Switch To Scenario*, kde vyberete požadovaný scénář. Pro nový scénář TCP nastavte jméno „TCP\_new\_connections“ a pro UDP „UDP\_new\_connections“. (Obr. 7.17)



Obr. 7.17: Duplikování scénáře.

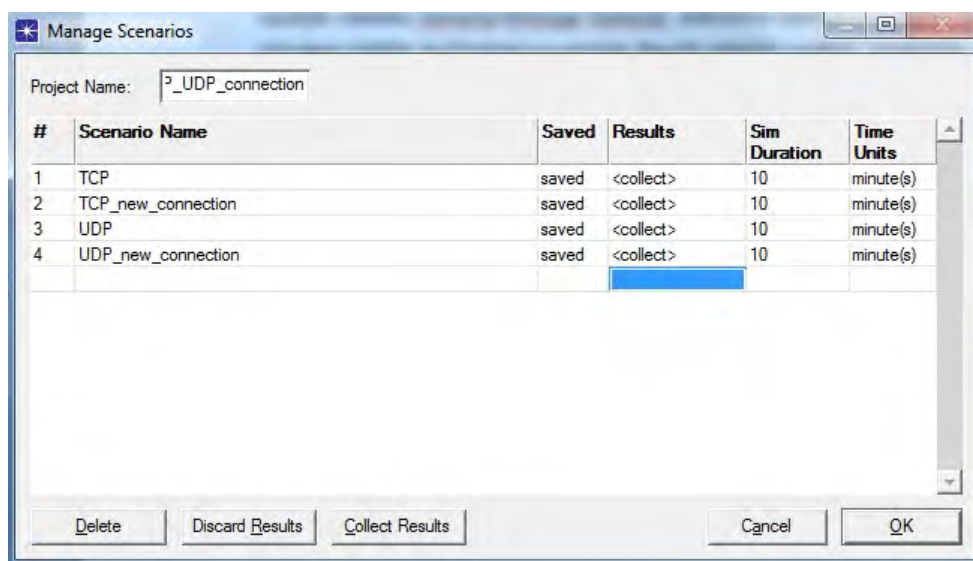
2. V nově vytvořených scénářích nastavte komponentu **Tasks** tak, aby se pro každý nový požadavek navazovalo nové spojení. Vstupte proto do konfigurace komponenty **Tasks**. V konfigurační nabídce vyberte *Task Specification/Manual*

*Configuration*. V okně *Manual Configuration* vyberte poslední položku *Transport Connection* a u položky *Policy* vyberte možnost „*New Connection per Request*“. (Obr. 7.18) Nastavení provedte pro oba nově vytvořené scénáře TCP\_new\_connection i UDP\_new\_connection.



Obr. 7.18: Nastavení nového spojení pro každý požadavek.

- Po dokončení konfigurace nových scénářů musíte pro získání výsledků spustit simulaci, k čemuž využijte nabídku *Scenario/Manage Scenario*. Jednotlivé scénáře si seřadte podle obrázku 7.19. Čas simulace změňte na 10 minut a u položek *Results* vyberte <collect> respective <recollect>. Po tomto nastavení potvrďte tlačítkem OK.



Obr. 7.19: Nastavení parametrů v *Manage Scenarios*.



### 7.3.2 Doplnující otázky a úkoly

- 1) Zobrazte si výsledky simulace a projděte si grafy.
- 2) Zobrazte si graf *Global Statistics/Custom Application/Traffic Sent* pro všechny 4 scénáře. Zobrazené grafy porovnejte a zdůvodněte. Proč u TCP došlo k výraznému prodloužení přenosu, zatímco přenos UDP zůstal stejný?
- 3) Zobrazte si graf *Object Statistics/subnet\_client/Traffic Sent* pro všechny 4 scénáře. U scénářů TCP klient odesílá jistá data, jaká data to jsou?

## 7.4 Úkol 3 – zahazování paketů

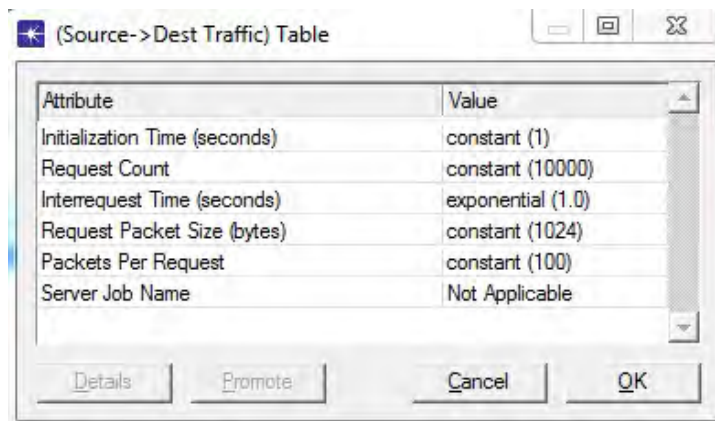
V tomto úkolu si vyzkoušíte chování transportních protokolů při nastavení určitého procenta zahazování paketů v komponentě *IP\_cloud*.

### 7.4.1 Postup

1. Současný projekt uložte (Ctrl+S) a pomocí *File/Save As...* si vytvořte kopii projektu, kterou budete dále upravovat. Zadejte nové jméno projektu „*Srovnani\_TCP\_UDP\_zahazovani*“.<sup>8</sup>
2. Odstraňte scénáře „TCP\_new\_connection“ a „UDP\_new\_connection“. Docílíte toho v *Scenarios/Manage Scenarios* označením příslušného scénáře a kliknutím na tlačítko *Delete*.
3. Ve scénářích „UDP“ a „TCP“ nastavte v komponentě *Tasks* zdrojová data podle obrázku 7.20. Pro provedení změny musíte vstoupit do editace nastavení komponenty (*Edit Attributes*) a v okně *Manual Configuration* vstoupit do konfigurace položky *Source->Dest Traffic*. V novém okně změňte počet požadavků (*Request Count*) na „10000“ a počet paketů v jednom požadavku (*Packets Per Request*) na „100“.

---

<sup>8</sup> Původní projekt zůstane uložený pod názvem „*Srovnani\_TCP\_UDP*“ a je možné se k němu vrátit. Projekt otevřete z hlavního okna programu pomocí *File/Open* a najdete projekt s požadovaným názvem.

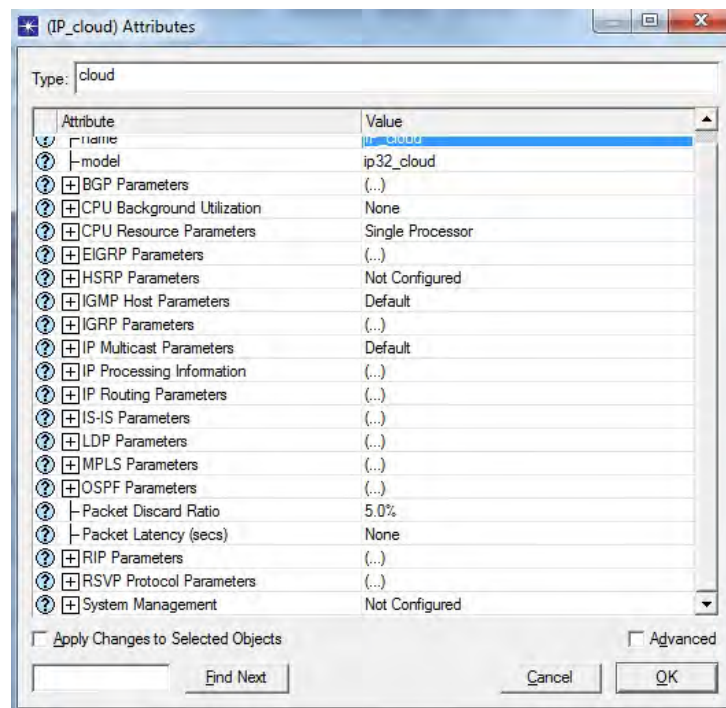


Obr. 7.20: Nastavení zdrojových dat.

4. Po nastavení nových zdrojových dat pro **oba** scénáře duplikujte scénář TCP a nazvěte ho „TCP\_zahazovani“. Duplikujte i upravený scénář UDP a nazvěte ho „UDP\_zahazovani“.
5. V nově vytvořených scénářích nastavte v komponentě *IP\_cloud* zahazování paketů na 5 %<sup>9</sup>. Docílíte toho vstoupením do konfigurace atributů (*Edit Attributes*) komponenty *IP\_cloud* a v poli *Packet Discard Ratio* vyberete hodnotu 5 %, viz Obr. 7.21. Zahazování paketů nastavte pro scénáře „TCP\_zahazovani“ i „UDP\_zahazovani“.

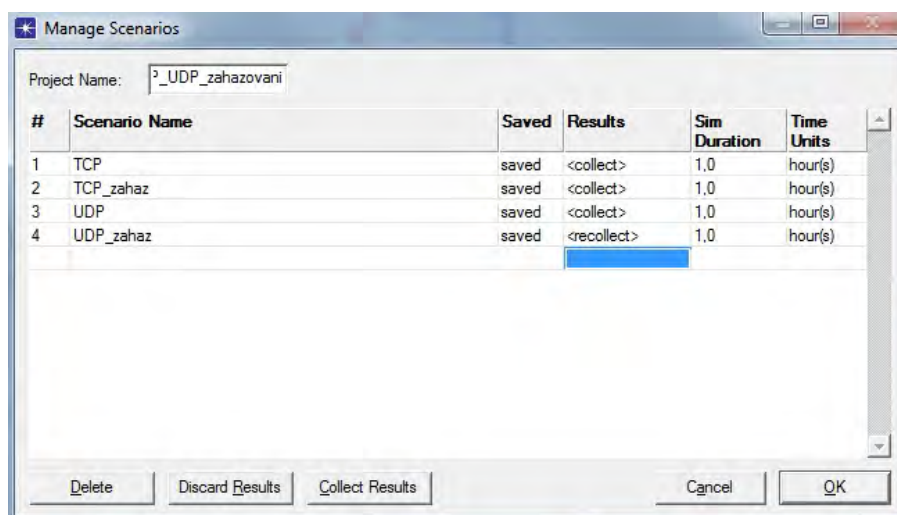
---

<sup>9</sup> V reálné síti se hodnota zahazování paketů pohybuje mezi hodnotami 10e-3 až 10e-9. Tato úloha má ale za cíl ukázat rozdíly mezi oběma protokoly, proto jsou nastavované hodnoty mnohonásobně větší.



Obr. 7.21: Nastavení zahazování paketů.

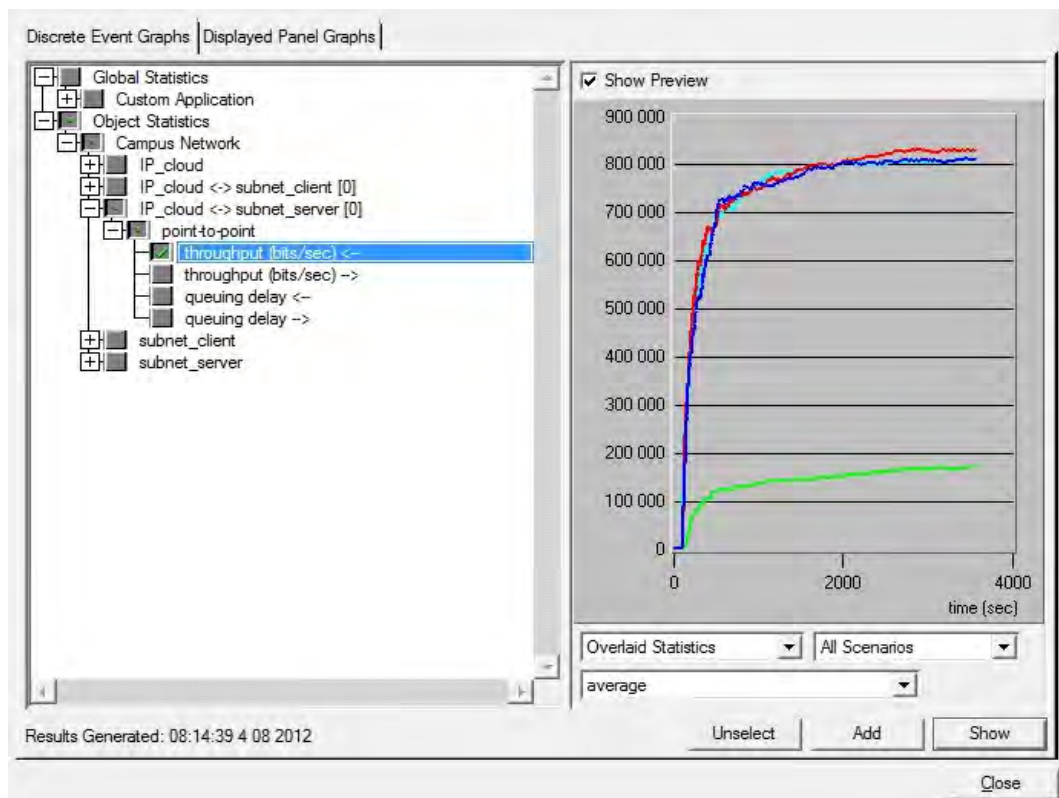
6. Po nastavení parametrů opět spusťte simulaci pro všechny scénáře pomocí položky menu *Scenarios/Manage Scenarios* (Obr. 7.22: Manage Scenarios. Délku simulace nastavte na 1 hodinu a u položky *Results* vyberte *<collect>* respective *<recollect>* pro všechny scénáře. Volbu potvrďte kliknutím na tlačítko *OK*.



Obr. 7.22: Okno *Manage Scenarios*.

Po dokončení simulace a zobrazení výsledků, konkrétně grafu *Object Statistics/Campus Network/subnet\_server <-> IP\_cloud/point-to-point/throughput (bit/sec)-->*

(graf znázorňující propustnost na lince směrem od serveru ke klientovi) byste měli získat shodnou statistiku s obrázkem. Pro zobrazení více scénářů do jednoho grafu je ještě nutné nastavit rolovací pole pod grafem (*Overlaid Statistics a All Scenario*). Zvolte průměrování hodnot *avarage* pro názornější zobrazení. Výsledný graf i s nastavenými parametry pro správné zobrazení grafu si můžete zkontrolovat podle obrázku 7.23.



Obr. 7.23: Výsledný graf propustnosti na lince směrem od serveru k IP\_cloud v bitech/s.

#### 7.4.2 Doplnující otázky a úkoly

- 1) Zobrazte si výsledky simulace a vyberte graf *Object Statistics/subnet\_server <- > IP\_cloud/point-to-point/throughput (bit/sec)-->*. Zobrazte si grafy pro všechny scénáře (*All Scenarios*). Všechny grafy si zobrazte do jednoho (*Overlaid Statistics*) a vyberte průměrování hodnot (*average*). Vysvětlete odlišné chování protokolů pro zahazování paketů. Vysvětlete výrazné snížení zatížení linky u TCP protokolu.

- 2) Scénář „TCP\_zahazovani“ duplikujte a měňte hodnotu zahazování paketů. Pokuste se najít hodnotu, kdy zahazování nebude mít vliv na zatížení linky.<sup>10</sup>

---

<sup>10</sup> Cílem tohoto úkolu by mělo být vytvoření několika nových scénářů, u kterých budete nastavovat různé velikosti chybovosti na komponentě IP\_cloud a budete pozorovat změnu zatížení linky. Ve výsledném grafu byste pak měli mít znázorněny scénáře s chybovostí např. 0, 1, 2, 3, 4 a 5 %.

## 8 SROVNÁNÍ WLAN S ETHERNETEM

### 8.1 Úvod k laboratorní úloze

Tato úloha je zaměřena na srovnání dvou přenosových technologií. Sítě typu WLAN jsou bezdrátové sítě a k šíření signálu používají elektromagnetické rádiové vlny v pásmech řádu GHz. Technologie Ethernet je zástupce síťových technologií používajících k přenosu strukturovanou kabeláž.

### 8.2 Úkol 1 – vytvoření topologie

V prvním úkolu této úlohy vytvoříte základní topologii se dvěma scénáři. V každém scénáři bude jeden server připojený Ethernetem ke směrovači. Client bude v jednom scénáři připojen technologií Ethernet a v druhém pomocí Wi-Fi.

#### 8.2.1 Popis vytvoření programu

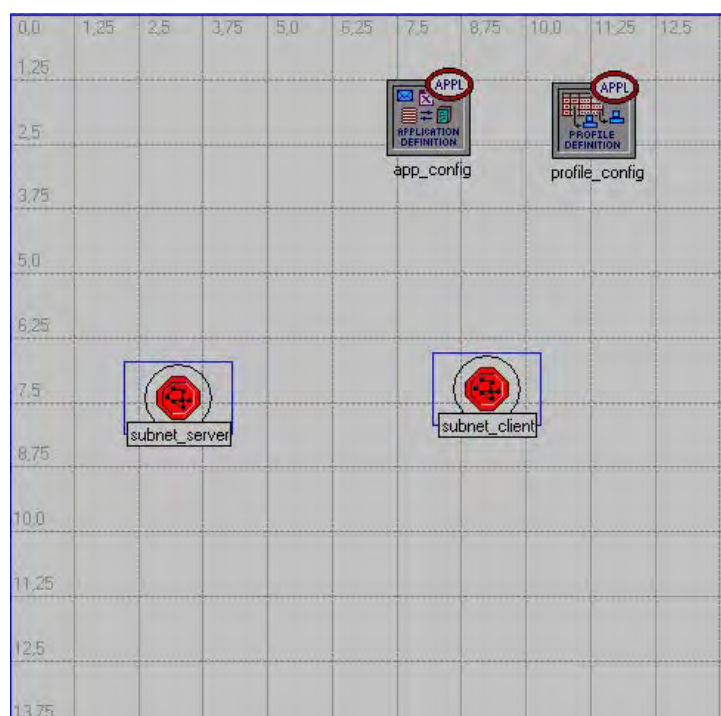
1. Spustíte program OPNET IT Guru Academic Edition.
2. Z menu programu vyberte položku **File/New...** (Ctrl + N) a v rolovací nabídce ponechejte „Project“ a potvrďte tlačítkem **OK**.
3. V následujícím okně zadejte jméno projektu a scénáře. Jméno projektu zvolte například „*Srovnani\_WLAN\_ethernet*“ (*Project Name*) a jméno scénáře „*ethernet*“ (*Scenario Name*).
4. Následně nechte vybranou položku „Create Empty Scenario“ a klikněte na **Next**.
5. Při výběru rozlohy označte položku „Campus“ a ponechejte zaškrtnuté „Use Metric Units“. Klikněte na **Next** a zadejte požadovanou rozlohu 14x14 kilometry.
6. V následujícím kroku máte na výběr několik technologií. Zatrhněte „ethernet\_advanced“, „routers“, „wireless\_lan“ a klikněte na **Next**. Poté potvrďte

volbou **OK** požadované nastavení, které si ještě jednou můžete zkontrolovat v přehledu.<sup>11</sup>

7. Vložte na plochu postupně tyto komponenty z okna *Object Palette*:

- I. Application Config
- II. Profile Config
- III. 2x subnet

Komponenty rozmístěte na plochu a pojmenujte podle obrázku 8.1.



Obr. 8.1: Základní topologie.

8. Dvojitým kliknutím na ikonu podsítě serveru (subnet\_server) vstupte do podsítě a z okna *Object Palette* vložte prvky „ethernet\_server\_adv“ a přepínač „ethernet4\_switch\_int“. Komponenty pojmenujte podle obrázku 8.2. Server

---

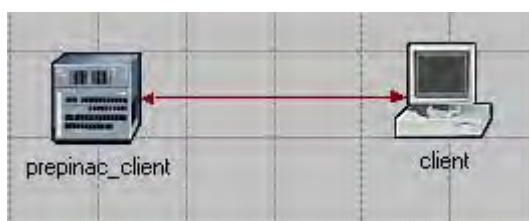
<sup>11</sup> Stejně jako při práci s jakýmkoliv jiným programem doporučuji práci průběžně ukládat (Ctrl + S). Při prvním uložení se program IT Guru dotáže, jestli opravdu chceme uložit projekt pod námi již definovaným názvem. Uložení je vhodné provádět vždy po změně či nastavení nějaké z komponent tak, aby se nastavené parametry zpřístupnili i pro nastavování dalších komponent.

a přepínač propojte technologií Ethernet 100baseT přetažením ikony 100baseT z okna Object Palette na pracovní plochu a prostým propojením obou komponent.<sup>12</sup>




Obr. 8.2: Podsít' serveru.

V dalším kroku proveďte konfiguraci pro klientskou podsít' (subnet\_client). Vložte přepínač „ethernet8\_switch\_int“ a stanici „ethernet\_wkstn\_adv“. Komponenty pojmenujte podle obrázku 8.3 a propojte technologií 10BaseT<sup>13</sup>. Propojení provedete přetažením ikony 10BaseT z okna Object Palette na pracovní plochu a prostým propojením obou komponent.



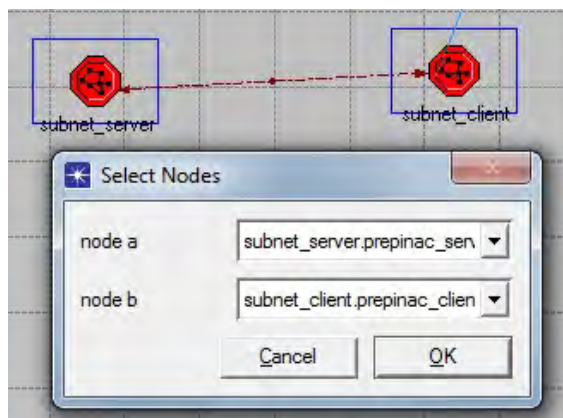
Obr. 8.3: Podsít' klienta.

9. Po nakonfigurování podsítí vstupte do nadřazené sítě a podsítě propojte technologií 100baseT. Po propojení se objeví nabídka s výběrem, které prvky z daných podsítí chcete propojit. V nabídce vyberte přepínač jak pro klientskou podsít', tak pro podsít' serveru. (Obr. 8.4)

<sup>12</sup> Pro přechod z podsítě do nadřazené sítě můžete použít ikonu , nebo klikněte na plochu pravým tlačítkem a z kontextového menu vyberte možnost „Go To Parent Subnet“.

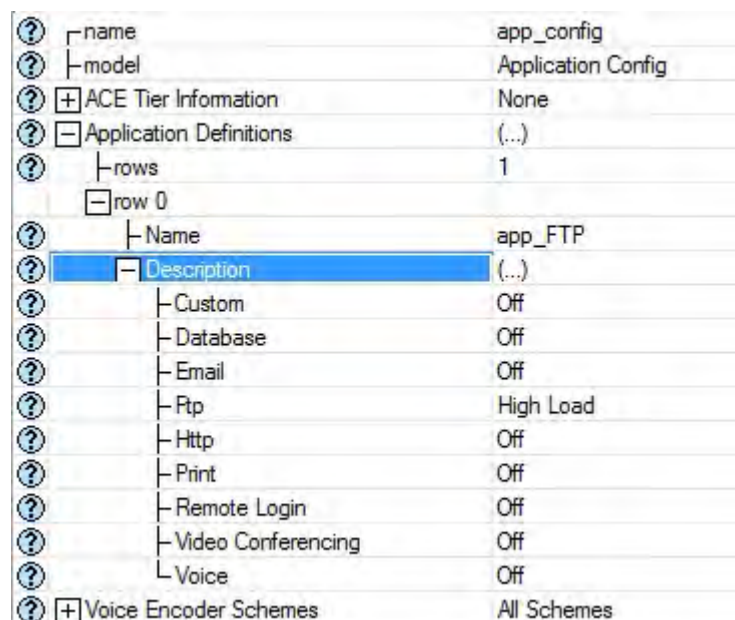
<sup>13</sup> Pro propojení klientů s přepínačem je využívána technologie 10BaseT z důvodu porovnávání technologie s bezdrátovou sítí WLAN, u které program OPNET umožňuje nastavit maximální rychlost na 11 Mbit/s. Pro ostatní spoje v síti společně pro scénáře WLAN i Ethernet je použita technologie 100BaseT.





Obr. 8.4: Okno výběru prvků pro propojení prvků v podsítích.

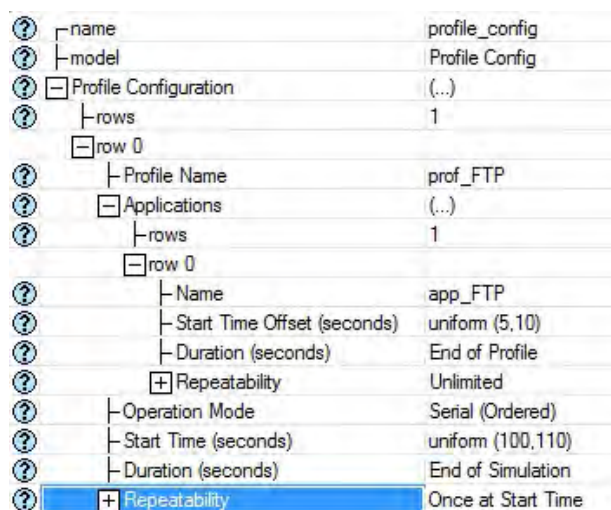
10. Nyní máte nakonfigurovanou základní topologii a přistoupíte k nastavování jednotlivých komponent. V prvním kroku budete nastavovat komponentu *Application Config*. V této komponentě se definují parametry aplikace. Vstupte do konfiguračního prostředí komponenty kliknutím pravým tlačítkem myši na ikonu a vybráním „*Edit Attributes*“. V záložce „*Application Definitions*“ nastavte *Rows* na 1 napište jméno aplikace „app\_FTP“. U položky *FTP* změňte typ zátěže na „*High Load*“, viz Obr. 8.5 a nastavení potvrďte tlačítkem **OK**.



Obr. 8.5: Nastavení aplikace FTP.

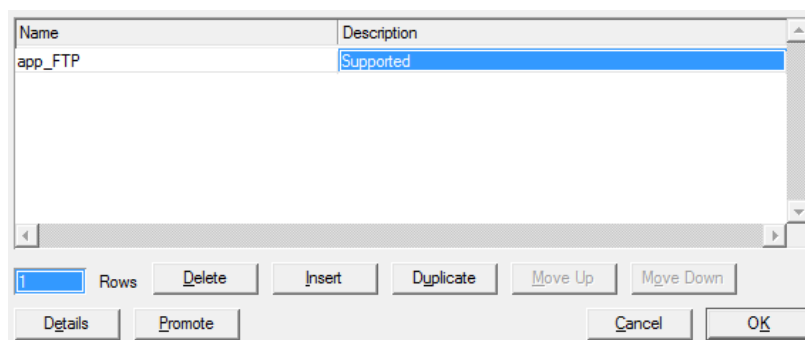
11. V dalším kroku pro nastavenou aplikaci vytvoříte profil pomocí *Profile Config*. Opět klikněte pravým tlačítkem na komponentu *Profile Config*, vyberte položku

„*Edit Attributes*“ a komponentu nastavte podle obrázku 8.6. Jméno profilu nastavte prof\_FTP a u jména aplikace vyberte vytvořenou aplikaci app\_FTP.



Obr. 8.6: Nastavení profilu pro aplikaci FTP.

12. Po nastavení aplikace a profilu musíte ještě zajistit podporu této aplikace a profilu na serveru a klientovi. Proto vstupte do konfigurace atributů (*Edit Attributes*) na **serveru**. V poli *Application: Supported Services* vyberte dříve definovanou aplikaci „app\_FTP“, viz Obr. 8.7.




Obr. 8.7: Podpora aplikace na serveru (*Supported Services*).

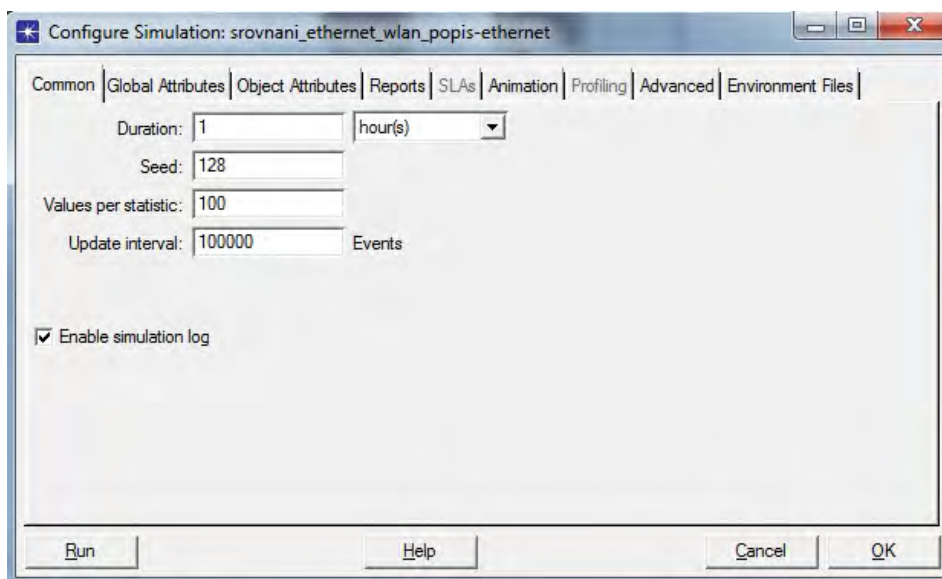
13. V dalším kroku provedete nastavení klienta. V poli *Application: Supported Profiles* nastavte dříve vytvořený profil „prof\_FTP“. Nastavení potvrďte a projekt uložte.
14. Po nakonfigurování základní topologie a jednotlivých komponent přistupte k vybrání statistik, které budete sledovat. Statistiku vyberete kliknutím pravého tlačítka myši na plochu a z nabídky vyberete *Choose Individual Statistics*. Většinu statistik budete nastavovat globálně pro celou síť. Statistiku u níž je v závorce

uvedeno, pouze client či server nastavte obdobným způsobem, ovšem pro vybrání statistiky pouze na požadovaném prvku, kliknete pravým tlačítkem myši na daný prvek a opět vyberete možnost *Choose Individual Statistics*.

Z nabízených statistik vyberte následující:

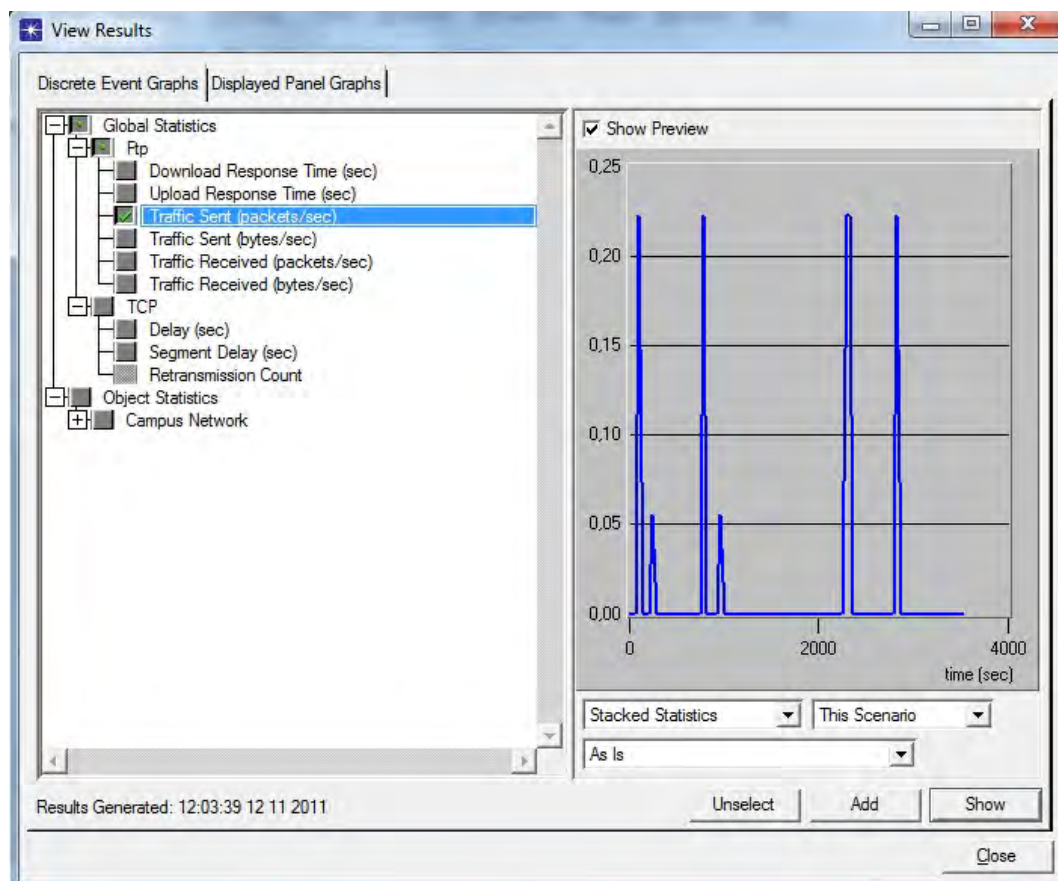
- a) Global Statistics: TCP  
FTP
- b) Node Statistics: TCP/Delay (sec)  
Server FTP (pouze server)  
Client FTP (pouze klient)
- c) Link Statistics: point-to-point/queuing delay -->  
point-to-point/queuing delay <--  
point-to-point/throughput (bits/sec) -->  
point-to-point/throughput (bits/sec) <--

15. Po vybrání sledovaných statistik můžete přistoupit k vlastní simulaci. Stisknutím ikony  (Run) se dostanete do konfiguračního okna simulace, kde nastavíte čas simulace na 1 hodinu, počet hodnot na statistiku 100 a obnovovací interval na 100000 hodnot. (Obr. 8.8) Po nastavení požadovaných parametrů stiskněte tlačítko **Run** pro zahájení simulace.



Obr. 8.8: Nastavení parametrů simulace.

16. Pro zobrazení výsledků klikněte pravým tlačítkem myši na plochu a z nabídky vyberte *View Results*. Po vybrání grafu z *Global Statistics/FTP* a zaškrtnutí políčka *Traffic Sent (packets/sec)* byste měli vidět graf shodný s obrázkem 8.9.<sup>14</sup>

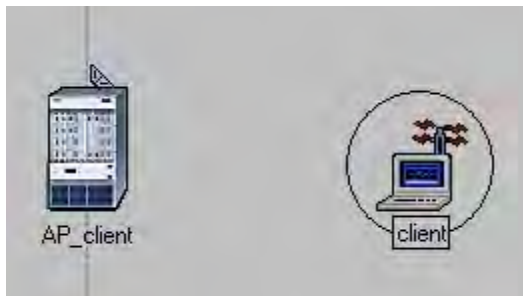


Obr. 8.9: Ukázka statistiky pro odeslaná data FTP v paketech/s.

17. Po úspěšném zobrazení grafu a ověření správnosti nakonfigurování jednotlivých prvků rozšířte projekt o další scénář. K vytvoření nového scénáře využijte možnost duplikování současného scénáře. Toho docílíte vybráním z menu *Scenarios/Duplicate Scenario* a zadáním jména nového scénáře. Nový scénář pojmenujte „wlan“.
18. V nově vytvořeném scénáři „wlan“ odstraníte oba objekty z podsítě klienta (subnet\_client) a nahradíte je ekvivalentními s podporou bezdrátového přenosu. Vstupte proto do podsítě client a odstraňte oba objekty. Jako přístupový bod vyberte

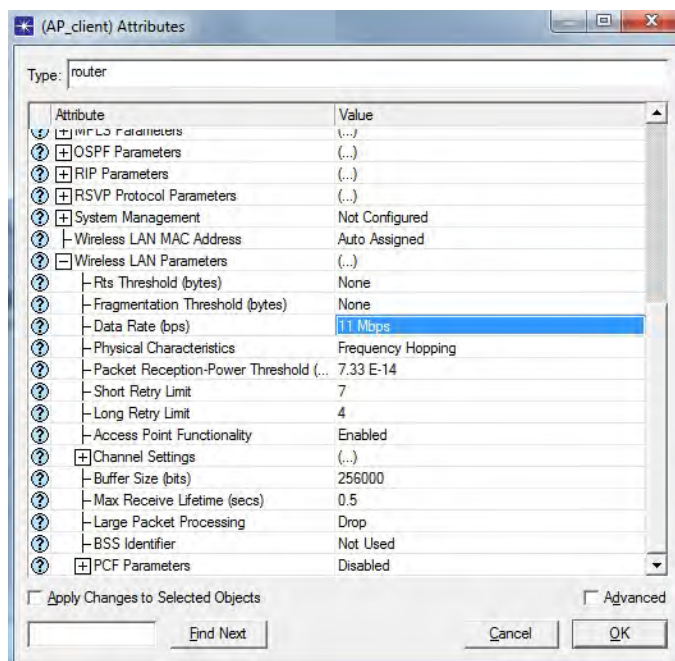
<sup>14</sup> Graf lze zobrazit po zmáčknutí tlačítka **Show** a v grafu pomocí kurzoru myši vybrat požadovanou oblast pro přiblížení. Pro navrácení zobrazení celého grafu můžete využít pravé tlačítko myši a vybrat „Full Horizontal Scale“ a „Full Vertical Scale“.

z *Object Palette* prvek „*wlan\_ethernet\_router (fix)*“ a jako klienta „*wlan\_wkstn (fix)*“. Klienta umístěte přibližně 100m od přístupového bodu a pojmenujte podle obrázku 8.10.



Obr. 8.10: Podsít' bezdrátového klienta.

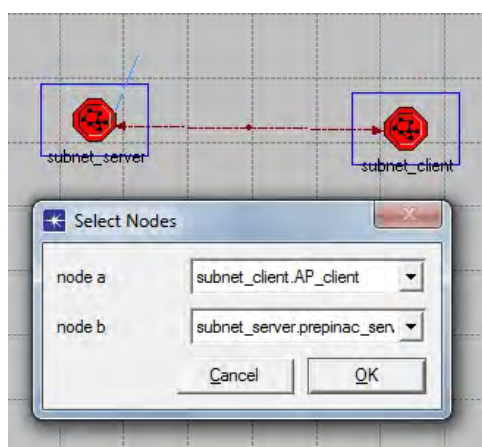
19. U obou prvků provedete nastavení přenosové rychlosti na 11Mb/s a u klienta navíc ještě musíte zvolit podporu FTP profilu. Nejprve vstupte do konfiguračního prostředí přístupového bodu (Edit Attributes) a vyberte položku *Wireless LAN Params*. V poli *Data Rate (bps)* nastavte na 11 Mbps<sup>15</sup>. (Obr. 8.11) Nastavení potvrďte a přejděte ke konfiguraci klienta.



Obr. 8.11: Nastavení přístupového bodu.

<sup>15</sup> Podpora nastavení přenosových rychlostí u bezdrátových sítí je v prostředí IT Guru značně omezena, proto se v úloze porovnává technologie 10BaseT s technologií WLAN o rychlosti 11 Mbit/s.

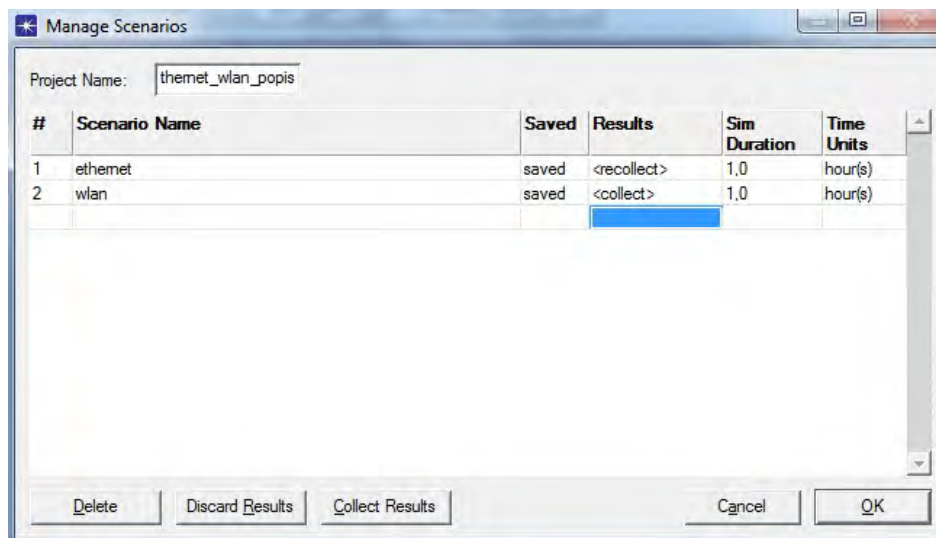
20. Na klientovi opět nastavte přenosovou rychlost na 11 Mbit/s a nastavte podporu dříve vytvořeného FTP profilu. V konfiguračním okně *clien*ta vyberte položku „*Wireless LAN Parametr*s“ a v pole „*Data Rate (bps)*“ nastavte na „11 Mbps“. V poli *Application: Supported Profiles* nastavte dříve vytvořený profil „prof\_FTP“. Nastavení potvrďte a projekt uložte.
21. K dokončení konfigurace scénáře „wlan“ ještě zbývá propojit obě podsítě. K propojení použijte technologii 100baseT. Po propojení podsítí se program dotáže, které prvky z podsítí chcete spojit. Vyberte přístupový bod na straně klientské podsítě a přepínač na straně podsítě serveru (Obr. 8.12).



Obr. 8.12: Propojení přístupového bodu s přepínačem.

22. Před vlastní simulací ještě zbývá vybrat statistiku pro nového klienta. Vstupte proto do podsítě klienta a klikněte pravým tlačítkem myši na klienta a vyberte položku *Choose Individual Statistics*. Z nabízených statistik vyberte *Client Ftp*.
23. Po nakonfigurování druhého scénáře je nutné znovu simulovat chování sítě. K tomu nyní nevyužívejte tlačítko Run jako v předchozím případě, ale vyberte z nabídky *Scenarios/Manage Scenarios...* a u položek *Results* vyberte <collect> respektive <recollect>. Délku simulace ponechte 1 hodinu a potvrďte volbu tlačítkem **OK**.





Obr. 8.13: Nastavení parametrů simulace.

### 8.2.2 Doplnující otázky a úkoly<sup>16</sup>

- 1) Zobrazte si výsledky simulace kliknutím pravého tlačítka myši na plochu a vybráním „View Results“. Pro zobrazení více položek do jednoho grafu vyberte „Overlaid Statistics“. Pro zobrazení všech scénářů vyberte hodnotu „All Scenarios“. U některých druhů statistik je vhodné zvolit průměrování hodnot „average“. Prohlédněte si jednotlivé nakonfigurované statistiky.
- 2) Ve výsledcích simulace si zobrazte graf *Global Statistics/TCP/Delay (sec)*. Porovnejte hodnoty pro Ethernet a WLAN.
- 3) Najděte další 2 statistiky, které ukazují rozdíly mezi přenosovými technologiemi.

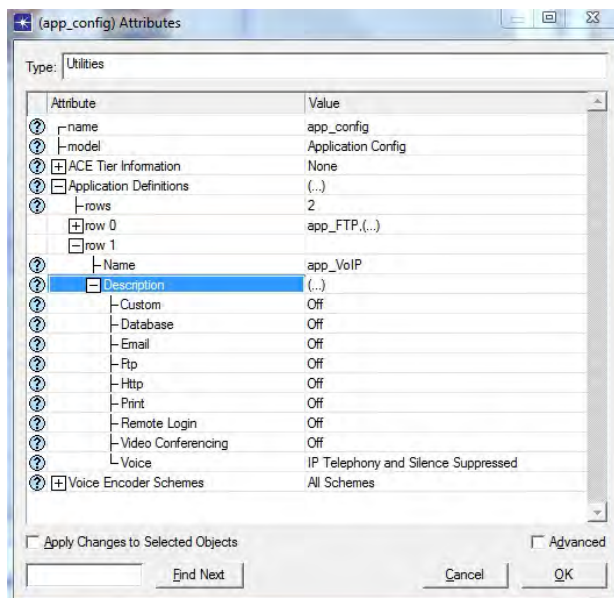
## 8.3 Úkol 2 – parametry WLAN v závislosti na vzdálenosti

V tomto úkolu se pokusíte najít vzdálenost, v které přestane komunikace mezi bezdrátovým klientem a přístupovým bodem v klientské podsíti. Budete vzdalovat bezdrátového klienta od přístupového bodu a určíte závislost sledovaných parametrů sítě na vzdálenosti.

<sup>16</sup> Odpovědi na otázky si poznamenejte a na konci cvičení je přednesete vyučujícímu.

### 8.3.1 Postup

1. Vytvořte si kopii projektu pomocí *File/Save As...* a zadejte nové jméno projektu „Srovnání\_WLAN\_ethernet\_ukol2“.<sup>17</sup>
2. Vytvořte si nový síťový provoz VoIP. V editaci komponenty „app\_config“ (*Edit Attributes*) přidejte novou aplikaci s názvem „app\_VoIP“ a nastavte u ní podporu „Voice/IP Telephony and Silence Suppressed“, viz Obr. 8.14.



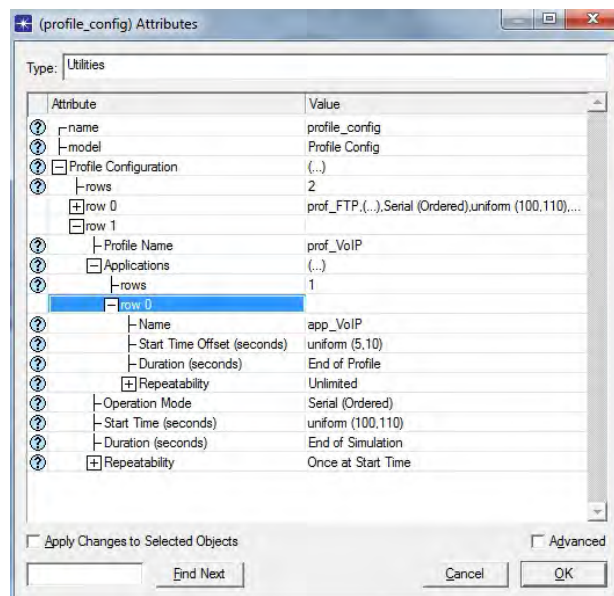
Obr. 8.14: Nastavení VoIP aplikace.

3. Po nastavení aplikace přidejte nový profil v editaci komponenty „profile\_config“ s názvem „prof\_VoIP“. V přidávaném profilu nastavte podporu aplikace „app\_VoIP“ v poli *Profile Configuration/row 1/Applications/row 0/Name*, viz Obr. 8.15.

---

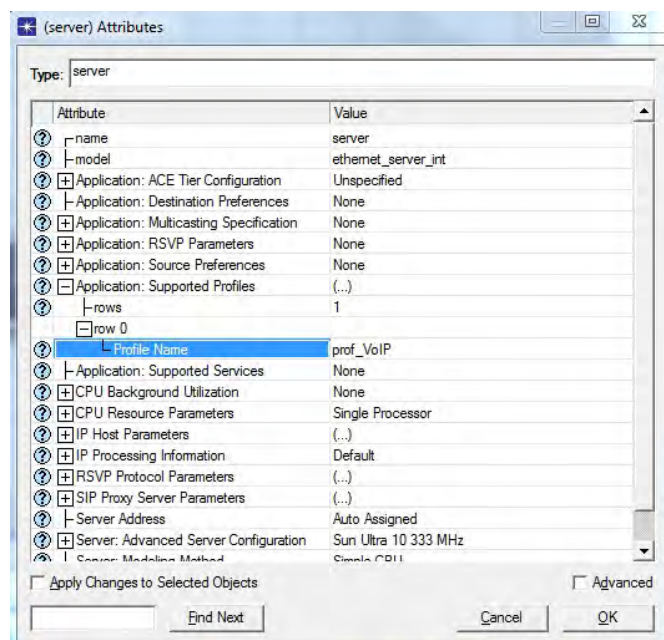
<sup>17</sup> Původní projekt zůstane uložený pod původním názvem „Srovnání\_WLAN\_ethernet“ a je možné se k němu vrátit. Projekt otevřete z hlavního okna programu pomocí *File/Open* a najdete požadovaný projekt.





Obr. 8.15: Nastavení profilu pro VoIP aplikaci.

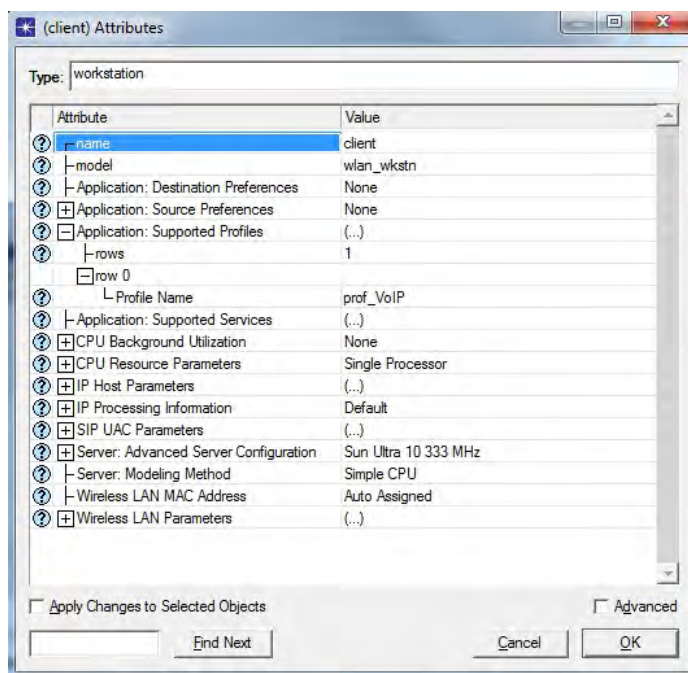
4. Vytvořený profil musíte povolit na serveru. Vstupte proto do editace parametrů serveru a v poli *Application:Supported Profiles/Profile Name* nastavte profil „prof\_VoIP“. V poli *Application:Supported Services* nastavte hodnotu *None*. Nastavení můžete vidět na obrázku 8.16.



Obr. 8.16: Nastavení podpory profilu VoIP na serveru.

5. V nastavení klienta opět vyberte podporu VoIP profilu „prof\_VoIP“ v poli

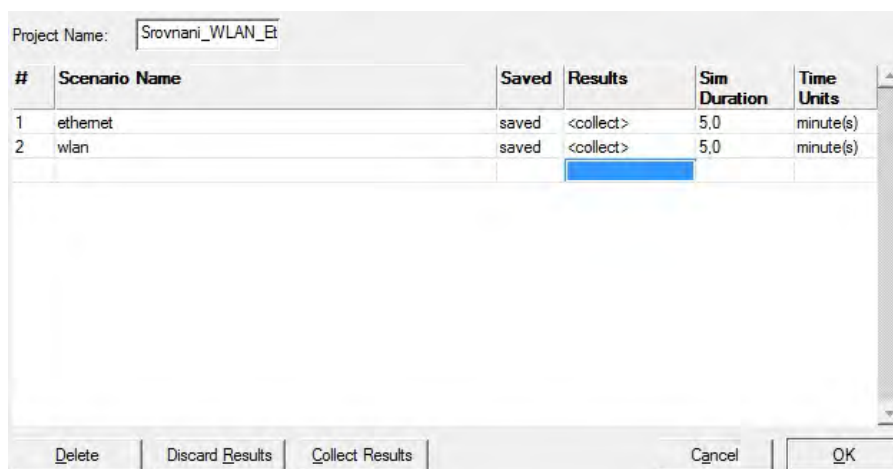
*Application:Supported Profiles/Profile Name.* V poli *Application:Supported Services* na klientovi nastavte podporu aplikace „app\_VoIP“.



Obr. 8.17: Nastavení klienta.

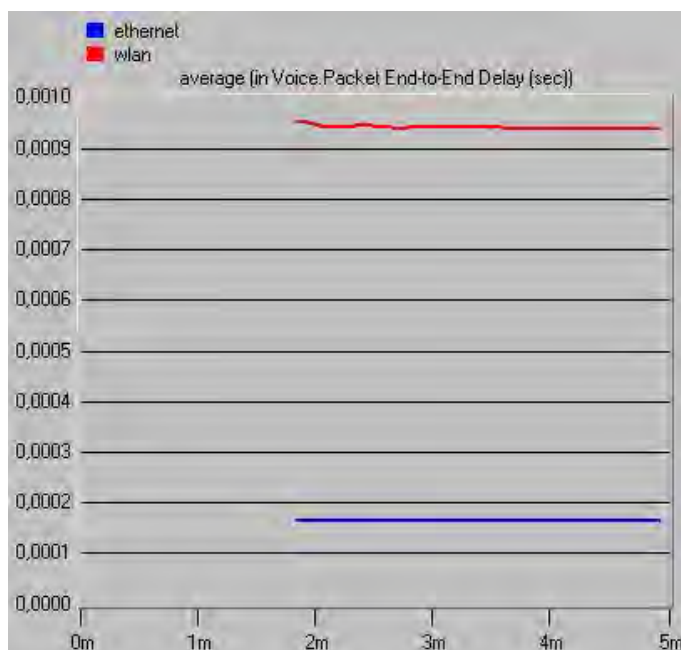
6. Nastavení VoIP aplikace a její podpory (položky 2 až 5 tohoto úkolu) proved'te pro oba scénáře (wlan a ethernet).
7. Po nakonfigurování obou scénářů vyberete statistiky, které budete sledovat. Statistiku vyberete kliknutím pravého tlačítka myši na plochu a z nabídky vyberete *Choose Individual Statistics*. „Node Statistics“ vyberte pouze na klientovi. Pro vybrání požadované statistiky pouze na určitém prvku, klikněte pravým tlačítkem myši na daný prvek a v nabídce *Choose Individual Statistics* statistiku zatrhněte. Z nabízených statistik vyberte následující:
  - a) Global Statistics: Voice/Packet Delay Variation  
Voice/Packet End-to-End Delay (sec)
  - b) Node Statistics: Voice Application/Packet Delay Variation  
Voice Application/Packet End-to-End Delay (sec)
 Statistiku musíte opět nakonfigurovat pro oba scénáře.
8. Po vybrání nových statistik musíte znovu simulovat chování sítě. K tomu využijte nabídku menu *Scenarios/Manage Scenarios...* a u položky *Results* vyberte *<collect>*

respektive *<recollect>*. Délku simulace nastavte na 5 minut a potvrďte volbu tlačítkem **OK**. (Obr. 8.18)



Obr. 8.18: Spuštění simulace.

9. K ověření správnosti nakonfigurování tohoto úkolu využijte statistiku *Global Statistics/Voice/Package End-to-End Delay (sec)* a porovnejte ji s obrázkem 8.19. Výsledky simulace zobrazíte kliknutím pravého tlačítka myši na plochu a výběrem možnosti *View Results*. Pro zobrazení obou grafů do jednoho využijte volbu *All Scenarios*, dále zvolte možnost zobrazení obou grafů do jednoho *Overlaid Scenarios* a průměrování hodnot *average*.



Obr. 8.19: Celkové zpoždění u WLAN a Ethernetu v s/min.

### 8.3.2 Doplnující otázky a úkoly

- 1) Z grafu celkového zpoždění (Obr. 8.19) vyvodte závěr jaký vliv má výběr přenosové technologie na celkové zpoždění hlasových služeb.
- 2) Vytvořte několik nových scénářů (cca 5) duplikováním scénáře „wlan“ a v každém scénáři nastavte odlišnou vzdálenost wlan klienta od přístupového bodu s krokem např. 300m. Vzdálenost nastavíte prostým posunutím klienta po ploše. K určení vzdálenosti využijte souřadnicový systém programu a funkci zoom. Cílem toho úkolu by mělo být experimentální určení maximálního komunikačního dosahu bezdrátového klienta.<sup>18</sup>
- 3) Ve výsledcích nově vytvořených scénářů pozorujte vliv přenosových parametrů (zejména statistiku *Voice Application/Packet End-to-End Delay* na klientovi) na vzdálenosti klienta od přístupového bodu.

## 8.4 Úkol 3 – rozšíření topologie

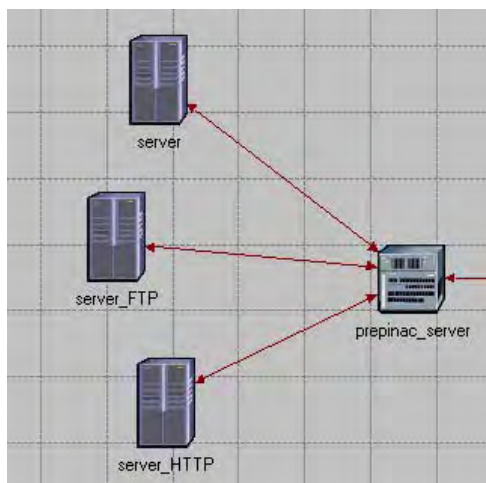
V tomto úkolu vytvoříte další síťový provoz kvůli dostatečnému vytížení sítě. Do scénáře přidáte 2 servery a 2 klienty, nastavíte nové aplikace a po nakonfigurování prvků a simulaci budete ve výsledných grafech porovnávat parametry sítě bez přidaného síťového provozu a s ním.

### 8.4.1 Postup

1. Vytvořte si kopii projektu pomocí *File/Save As...* a zadejte nové jméno projektu „Srovnání\_WLAN\_ethernet\_ukol3“.
2. Pomocí menu *Scenarios/Manage Scenarios* odstraňte všechny scénáře, kromě původních „ethernet“ a „wlan“.
3. Duplikujte scénář „ethernet“ pojmenujte ho „ethernet\_high\_load“.
4. V podsíti serveru v nově vytvořeném scénáři z Object Palette vložte 2 nové servery „ethernet\_server\_adv“. Rozmístěte a propojte s přepínačem technologií 100BaseT. Servery pojmenujte „server\_FTP“ a „server\_HTTP“, viz Obr. 8.20.

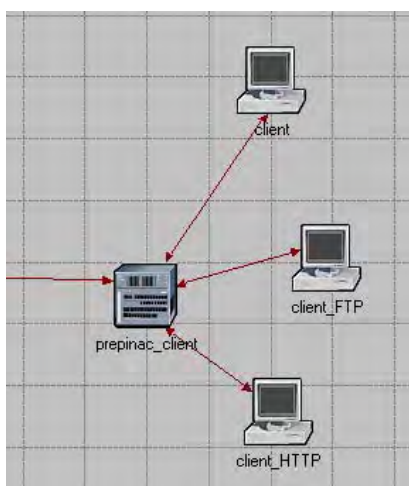
---

<sup>18</sup> K rozpoznání jestli klient stále komunikuje s přístupovým bodem, musíte daný scénář simulovat. V případě, že komunikace mezi bezdrátovým klientem a přístupovým bodem byla neúspěšná, nezobrazí se pro daný scénář žádné výsledky simulace.



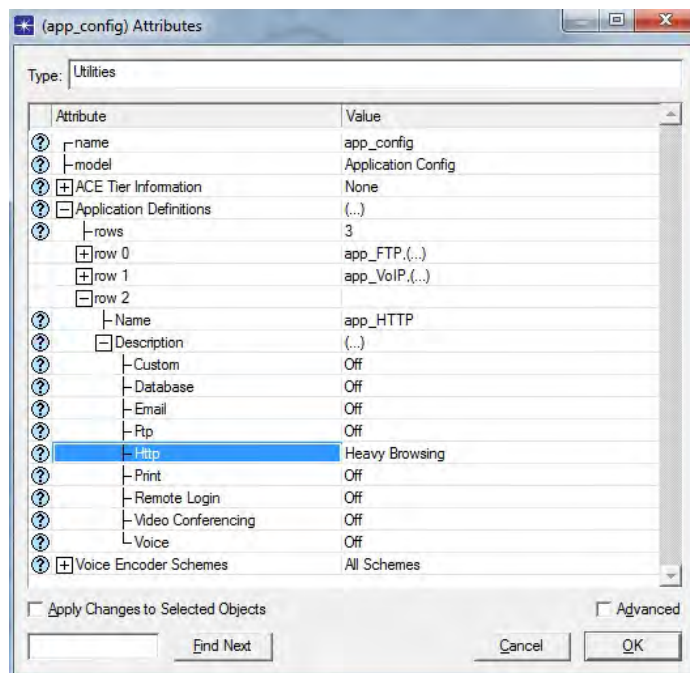
Obr. 8.20: Rozšířená podsíť serveru.

5. Vstupte do podsítě klienta a z Object Palette vložte 2 nové klienty „ethernet\_wkstn\_adv“. Klienty propojte s přepínačem technologií 10BaseT a pojmenujte je „client\_HTTP“ a „client\_FTP“. (Obr. 8.21)



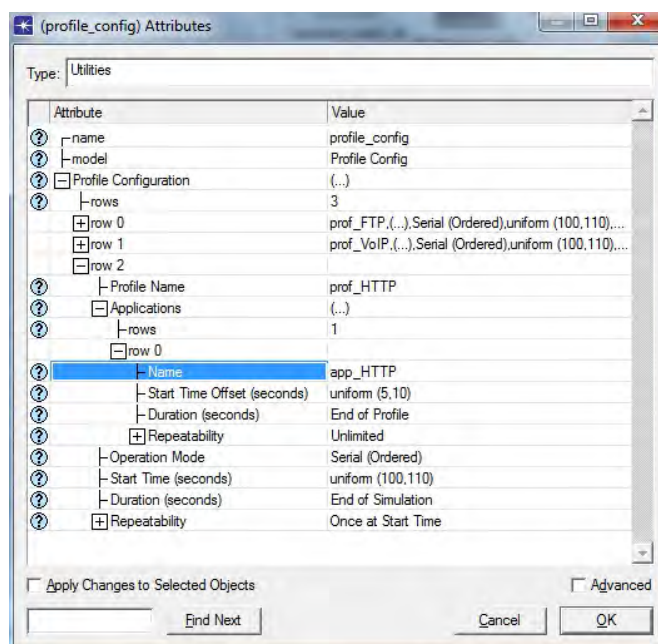
Obr. 8.21: Rozšířená podsíť klientů.

6. Aplikace FTP a VoIP již máte nastaveny z předchozích úkolů, zbývá přidat třetí aplikaci http. Vstupte proto do nastavení parametrů komponenty „app\_config“ a nastavte novou aplikaci s názvem „app\_HTTP“ podle obrázku 8.22. U položky http nastavte „Heavy Browsing“.



Obr. 8.22: Přidání HTTP aplikace.

- Pro novou aplikaci nastavte nový profil „prof\_HTTP“ podle obrázku 8.23.



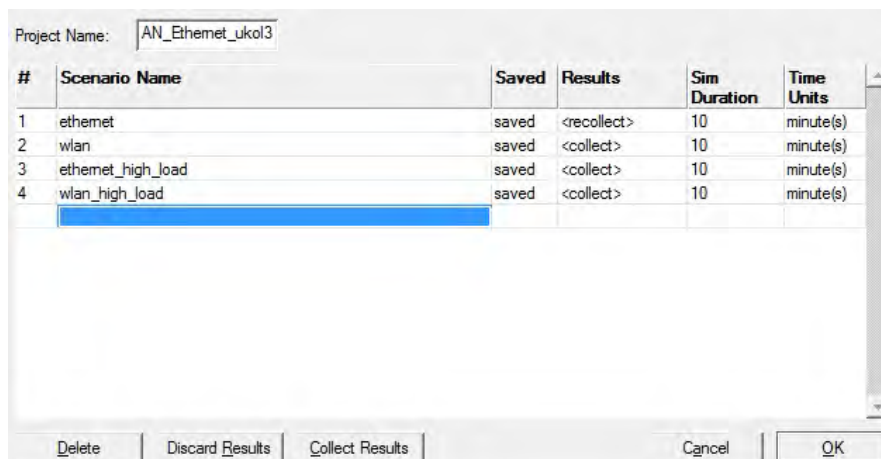
Obr. 8.23: Nastavení/přidání HTTP profilu.

- V serverové pod síti nastavte podporu aplikací na jednotlivých serverech. Pro „server\_FTP“ vstupte do konfigurace parametrů a v poli *Application: Supported*

*Services* vyberte „app\_FTP“. Pro server http postupujte shodně, jen vyberte hodnotu „app\_HTTP“.

9. Po nastavení podpory na serverech zbývá ještě nastavit podporu těchto aplikací na klientech. Vstupte proto do klientské podsítě. Pro „client\_FTP“ nastavte v *Application: Supported Profiles* profil „prof\_FTP“. Pro „client\_HTTP“ nastavte v *Application: Supported Profiles* profil „prof\_HTTP“.
10. Duplikujte scénář „wlan“, pojmenujte ho „wlan\_high\_load“ a opakujte kroky 4 až 9 tohoto úkolu i pro scénář „wlan\_high\_load“ s následujícími úpravami. Konfigurace je totožná, pouze v pátém kroku vložíte bezdrátové klienty „wlan\_wkstn (fix)“. Bezdrátové klienty vložte do vzdálenosti 100m od přístupového bodu a na klientech nastavíte přenosovou rychlost na 11 Mbit/s. Pro nastavení přenosové rychlosti u klientů vstupte do konfigurace parametrů (Edit Attributes) a v poli *Wireless LAN Params/Data Rate (bps)* vyberete 11Mbps.
11. Po nakonfigurování obou scénářů vyberete statistiky, které budete sledovat. „Node Statistics“ vyberte pouze na klientovi, který dané aplikace podporuje. Pro vybrání požadované statistiky pouze na určitém prvku, klikněte pravým tlačítkem myši na daný prvek a v nabídce *Choose Individual Statistics* statistiku zatrhněte. Statistiky musíte vybrat v každém scénáři zvlášť. Z nabízených statistik vyberte následující:
  - a) Node Statistics: Client Http (pouze client\_HTTP)Statistiku opět musíte nastavit na klientovi pro oba scénáře samostatně.
12. Po vybrání nových statistik musíte znovu simulovat chování sítě. K tomu využijte nabídku menu *Scenarios/Manage Scenarios...* a u položky *Results* vyberte <collect> respective <recollect>. Délku simulace nastavte na 10 minut a potvrďte volbu tlačítkem **OK**, viz Obr. 8.24.





Obr. 8.24: Manage Scenarios.

### 8.4.2 Doplnující otázky a úkoly<sup>19</sup>

- 1) Zobrazte si výsledky simulace kliknutím pravého tlačítka myši na plochu a vybráním *View Results*. Pro zobrazení více položek do jednoho grafu vyberte *Overlaid Statistics*. Pro zobrazení všech scénářů vyberte hodnotu *All Scenarios*. U některých druhů statistik je vhodné zvolit průměrování hodnot *average*. Pozornost věnujte zejména statistikám na klientech. Vyberte 2 statistiky, které ukazují rozdíly mezi bezdrátovou sítí a Ethernetem.
- 2) Vyberte statistiku pro *Campus Network/subnet\_client/client/Voice Application/Packet End-to-End Delay* a porovnejte průběh pro různé scénáře.

<sup>19</sup> Pro některé statistiky je nutné si určitou část grafu přiblížit. Přiblížení části grafu lze provést výběrem myši požadované části grafu po zobrazení grafu tlačítkem **Show**.



## 9 SMĚROVACÍ PROTOKOLY

### 9.1 Úvod k laboratorní úloze

Laboratorní úloha je zaměřena na směrovací protokoly patřící do skupiny IGP (*Interior Gateway routing Protocol*), tedy protokoly působící uvnitř jednoho autonomního systému. V laboratorní úloze se seznámíte se dvěma zástupci směrovacích protokolů RIP (*Routing Information Protocol*) a OSPF (*Open Shortest Path First*).

### 9.2 Úkol 1 – vytvoření topologie, simulace RIP

V první části úlohy vytvoříte základní scénář s topologií sítě, ze které budete vycházet ve všech dalších scénářích. V úvodním scénáři budete využívat směrovací protokol RIP, který je v jeho první verzi přednastaven jako výchozí v programu IT Guru. Součástí prvního úkolu bude též vytvoření druhého scénáře se stejnou topologií, ale se směrovacím protokolem RIPv2.

#### 9.2.1 Popis vytvoření programu

1. Spustíte program OPNET IT Guru Academic Edition.
2. Z menu programu vyberte položku **File/New...** (Ctrl + N) a v rolovací nabídce ponechejte „Project“ a potvrďte tlačítkem **OK**.
3. V následujícím okně zadejte jméno projektu a scénáře. Jméno projektu zvolte například „RIP\_OSPF“ (*Project Name*) a jméno scénáře „RIP“ (*Scenario Name*).
4. Následně nechte vybranou položku „Create Empty Scenario“ a klikněte na **Next**.
5. Při výběru rozlohy označte položku „Campus“, ponechejte zaškrtnuté „Use Metric Units“ a klikněte na **Next**.
6. Nyní zadáváte požadovanou rozlohu, kterou ponechejte na výchozích hodnotách, tedy 10x10 km.



7. V následujícím kroku máte na výběr několik technologií. Zatrhněte „internet toolbox“ a „utilities“ klikněte na **Next**. Poté potvrďte volbou **OK** požadované nastavení, které si ještě jednou můžete zkontrolovat v přehledu.<sup>20</sup>
8. Vložte na plochu postupně tyto komponenty z okna *Object Palette*:
  - I. 9x ethernet4\_slip8\_gtwy
  - II. 1x subnet
9. Komponenty rozmístěte na plochu a pojmenujte podle obrázku 9.1. Přejmenování prvku provedete kliknutím pravým tlačítkem myši na daný prvek a z kontextového menu vyberete možnost *Set Name*.



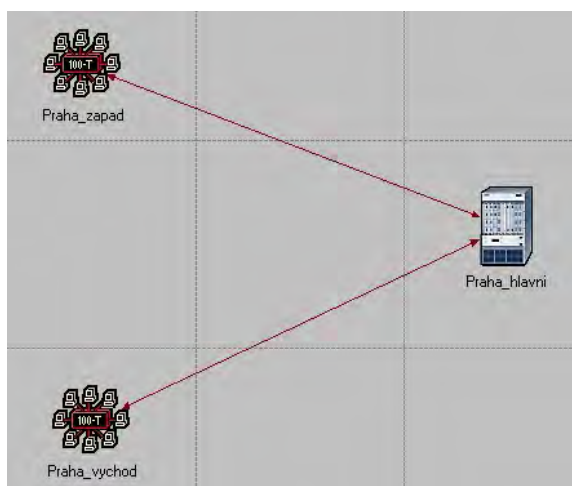
Obr. 9.1: Základní topologie úlohy bez propojení.

10. Dvojitým kliknutím na ikonu „podsit\_Praha“ vstupte do podsítě a z okna *Object Palette* vložte směrovač „ethernet4\_slip8\_gtwy“ a 2x „100BaseT\_LAN“, což je

<sup>20</sup> Stejně jako při práci s jakýmkoliv jiným programem doporučuji práci průběžně ukládat (Ctrl + S). Při prvním uložení se program IT Guru dotáže, jestli opravdu chcete uložit projekt pod již definovaným názvem při zakládání projektu. Uložení je vhodné provádět vždy po změně či nastavení nějaké z komponent, tak aby se nastavené parametry zpřístupnili i pro nastavování dalších komponent.

<sup>21</sup> Ve vytvořeném projektu můžete tlačítka  a  vybrat požadovanou oblast.

komponenta simulující ethernetovou LAN síť složenou z několika klientů a serveru (defaultně 10 klientů a jeden server). Komponenty pojmenujte podle obrázku 9.2. Směrovač s prvkem „100BaseT\_LAN“ propojte technologií Ethernet 100BaseT přetažením ikony „100BaseT“ z okna *Object Palette* na pracovní plochu a prostým spojením obou komponent.<sup>22</sup>




Obr. 9.2: Podsít Praha.

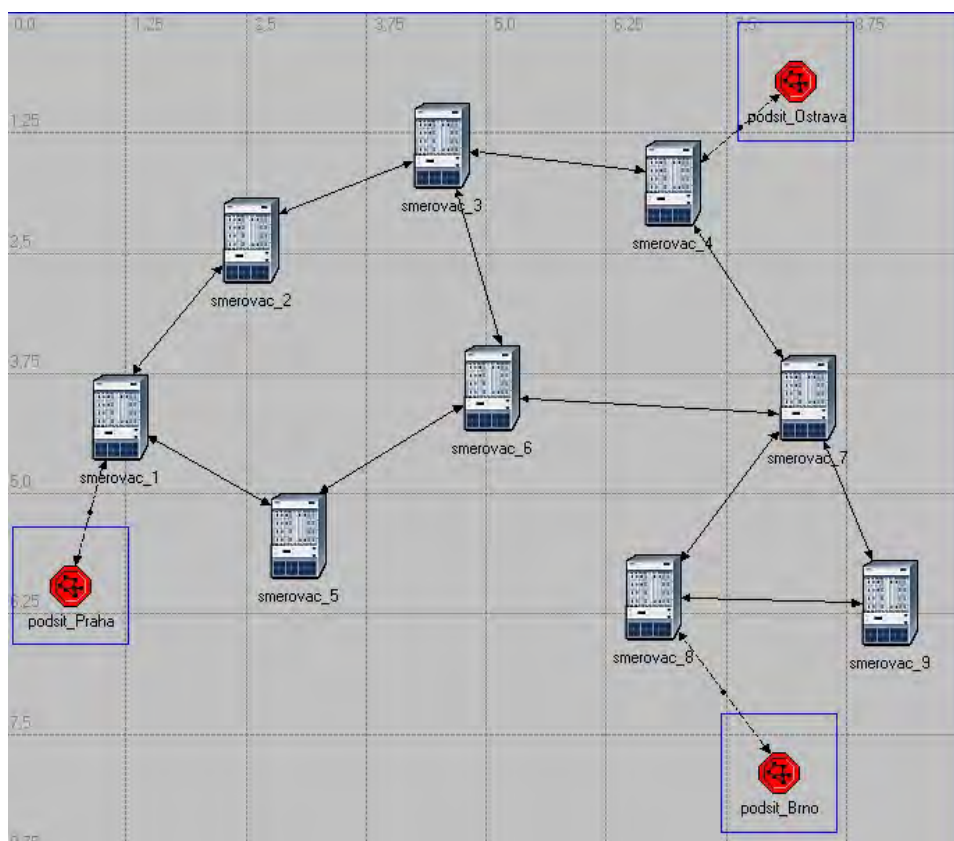
Na směrovači uvnitř podsítě vstupte do jeho nastavení, čehož docílíte pravým kliknutím na ikonu a z kontextového menu vyberete *Edit Attributes*. Z nabídky vyberete *IP Routing Parametr*s a u položky *Routing Table Export* zvolíte možnost *Once at End of Simulation*. Tímto krokem zajistíte vygenerování směrovací tabulky pro daný směrovač po skončení simulace.

11. V dalším kroku vytvoříte 2 další podsítě (podsit\_Brno a podsit\_Ostrava), k čemuž využijte duplikování podsítě podsit\_Praha (Ctrl+c, Ctrl+v). U obou nově vytvořených podsítí změňte název podsítě i jednotlivých prvků uvnitř podsítě. Např. pro „podsit\_Brno“ směrovač pojmenujte „Brno\_hlavni“ a komponenty zastupující síť LAN jako „Brno\_vychod“ a „Brno\_zapad“. Celková topologie včetně nově vytvořených podsítí je na obrázku 9.3.

---

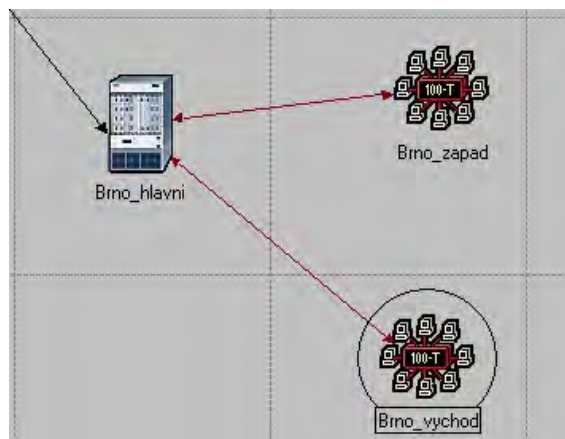
<sup>22</sup> Pro přechod z podsítě do nadřazené sítě můžete použít tlačítko , nebo klikněte na plochu pravým tlačítkem a z kontextového menu vyberte možnost „Go To Parent Subnet“.

12. Pro dokončení základní topologie ještě zbývá propojit směrovače mezi sebou. Propojení provedte technologií PPP DS3 prostým přetažením ikony „PPP\_DS3“ z okna *Object Palette* na plochu a propojením požadovaných komponent. Propojení realizujte podle obrázku 9.3.



Obr. 9.3: Kompletní topologie úlohy.

Propojení objektu uvnitř podsítě s objektem vně podsítě provedete v nadřazené síti propojením dané podsítě s požadovaným objektem. Po propojení se program zeptá, se kterým objektem uvnitř podsítě chcete spojit, a nabídne možnosti, z kterých vyberete vámi požadovaný objekt. Budete tedy propojovat například objekty „směrovac\_8“ s „podsit\_Brno“ a při dotazu programu zvolíte možnost podsit\_Brno.Brno\_hlavni. U ostatních podsítí budete posupovat obdobně. Propojení uvnitř podsítě je pro ilustraci znázorněno na obrázku 9.4.



Obr. 9.4: Podsít' Brno včetně spoje ke směrovači 8.

13. Na směrovači „*smerovac\_6*“ vstupte do konfigurace směrovače (*Edit Attributes*). Z nabídky vyberete *IP Routing Parametrs* a u položky *Routing Table Export* zvolíte možnost *Once at End of Simulation*. Tímto nastavením zpřístupníte směrovací tabulku na daném směrovači po skončení simulace.
14. Na směrovačích uvnitř každé z podsítí (Praha, Brno a Ostrava) budete nastavovat IP adresy<sup>23</sup> na rozhraních IF0 a IF1, ke kterým jsou připojeny komponenty „*100BaseT\_LAN*“. Přiřazovat budete adresy podle tabulky 9.1. Pro nastavení požadovaných adres vstupte do nastavení daného směrovače (*Edit Attributes*) uvnitř podsítě. Dále z nabídky vyberte položku *IP Routing Paramters/Interface Information* a přenastavte IP adresy podle obrázku 9.5, na kterém je znázorněno nastavení pro směrovač „*Praha\_hlavni*“ uvnitř podsítě „*podsit\_Praha*“. Na směrovačích uvnitř ostatních podsítí bude nastavení obdobné, jen přiřadíte správné IP adresy podle tabulky 9.1.

Tab. 9.1: IP adresy směrovačů pro připojení simulovaných LAN sítí.

Simulovaná LAN	IP adresa/maska směrovače
Praha_vychod	10.10.10.1/255.255.255.0
Praha_zapad	10.10.20.1/255.255.255.0
Brno_vychod	150.10.10.1/255.255.255.0
Brno_zapad	150.10.20.1/255.255.255.0

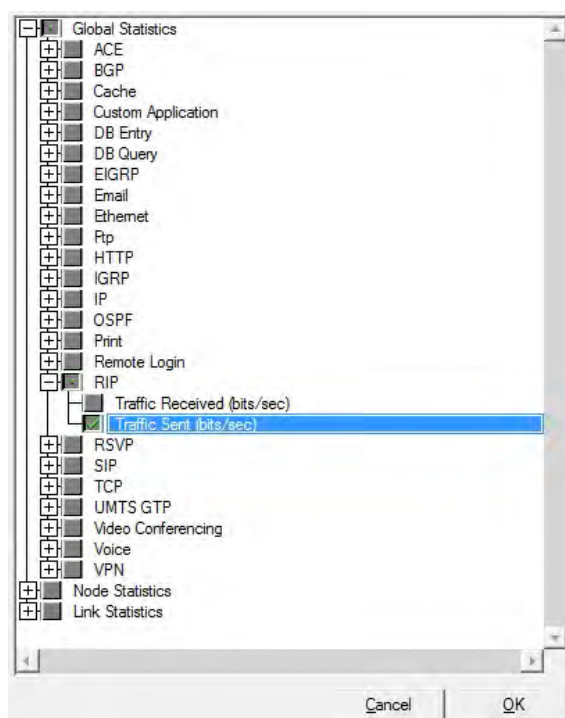
<sup>23</sup> Pro zjištění, na které rozhraní směrovače je připojena daná simulovaná LAN najedte kurzorem myši na spoj mezi směrovač a daným objektem. Objeví se kontextová nápověda popisující daný spoj.

Ostrava_vychod	172.16.10.1/255.255.255.0
Ostrava_zapad	172.16.20.1/255.255.255.0


Attribute	Value
Router ID	Auto Assigned
Autonomous System Number	Auto Assigned
Interface Information	(...)
rows	12
+ row 0	IF0,Active,10.10.10.1,255.255.255.0,Not Used,...
+ row 1	IF1,Active,10.10.20.1,255.255.255.0,Not Used,...
+ row 2	IF2,Active,Auto Assigned,Auto Assigned,Not Us...
+ row 3	IF3,Active,Auto Assigned,Auto Assigned,Not Us...

Obr. 9.5: Nastavení IP adres pro směrovač Praha\_hlavni.

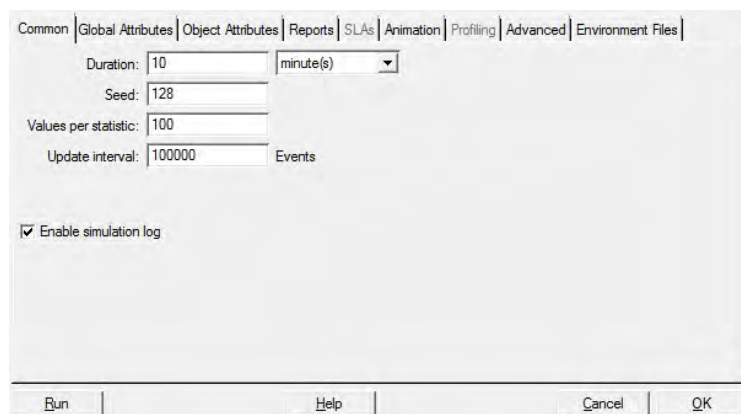
15. Před spuštěním simulace vyberete statistiku zobrazující RIP provoz během simulace. Statistiku vyberete kliknutím pravého tlačítka myši na plochu a výběrem *Choose Individual Statistics*. V nově otevřeném okně *Choose Results* vyberete v *Global Statistics/RIP* položku *Traffic Sent (bits/sec)*. (Obr. 9.6)



Obr. 9.6: Nastavení statistiky RIP.

16. Stisknutím ikony  (Run) se dostanete do konfiguračního okna simulace, kde v záložce *Common* změníte délku simulace na 10 minut, ostatní parametry v této

záložce ponechejte, viz obrázek 9.7. V záložce *Global Attributes* nastavte položku *IP Dynamic Routing Protocol* na *RIP*, u položky *IP Interface Addressing Mode* vyberte *Auto Addressed/Export* a u *RIP Sim Efficiency* vyberte *Disabled*. Touto volbou zajistíte fungování RIP protokolu během celé doby simulace, nejen po přednastavenou dobu. Pro spuštění simulace stiskněte tlačítko **Run**.



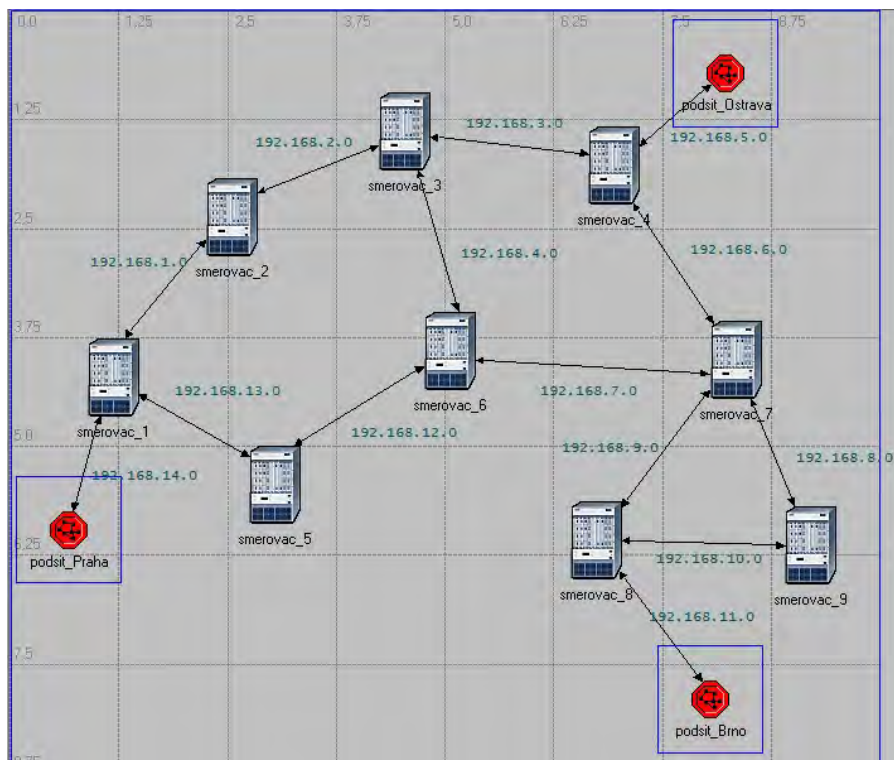
Obr. 9.7: Nastavení parametrů simulace.

17. Po dokončení simulace ukončete simulační okno kliknutím na tlačítko **Close**. Můžete si prohlédnout vyexportovaný soubor s přiřazenými IP adresy. Nejdříve vyberte položku menu *File/Model Files* a vyberte možnost *Refresh Model Directories*. Po obnovení adresáře zvolte položku *File/Open...* a v rolovací nabídce zvolte *Generic Data File*. Nyní již stačí ze seznamu vybrat požadovaný soubor *RIP\_OSPF-RIP-ip\_addresses*. V tomto souboru je souhrn všech přiřazených IP adres, který můžete využít později při orientaci ve směrovacích tabulkách.<sup>24</sup>

---

<sup>24</sup> Pro lepší orientaci ve směrovacích tabulkách lze IP adresy z vygenerovaného souboru ručně napsat k jednotlivým spojům výběrem z menu *Topology/Open Annotation Palette*, viz Obr. 9.8. Do textového okna vepíšete síťovou adresu, kterou zjistíte z vygenerovaného souboru s IP adresami pro daný spoj. IP adresy přiřazené na obrázku 9.8 jsou pouze orientační.





Obr. 9.8: Ukázka topologie s vepsanými IP adresami, které mohou být odlišné.

18. Směrovací tabulky uvidíte pro všechny 3 směrovače uvnitř jednotlivých podsítí a pro „smervac\_6“. Směrovací tabulky pro ostatní směrovače v topologii by vypadaly podobně, samozřejmě s odlišnými metrikami pro jednotlivé adresy. Směrovací tabulky si zobrazíte kliknutím pravým tlačítkem myši na plochu a výběrem možnosti *Open Simulation Log*. V okně *Log Browser* již můžete vybrat jednu ze směrovacích tabulek kliknutím do oblasti *Message*. Výstup ze směrovací tabulky by měl vypadat podobně jako na obrázku 9.9, kde je znázorněna směrovací tabulka pro směrovač „Praha\_hlavní“. Směrovací tabulky si prostudujte a seznamte se s položkami uloženými uvnitř směrovacích tabulek. Prozatím jste nakonfigurovali pouze scénář pro první verzi RIP protokolu, proto je dobré si uvědomit, že jsou ve směrovací tabulce uvedeny pouze *classful* adresy.



COMMON ROUTE TABLE snapshot for:

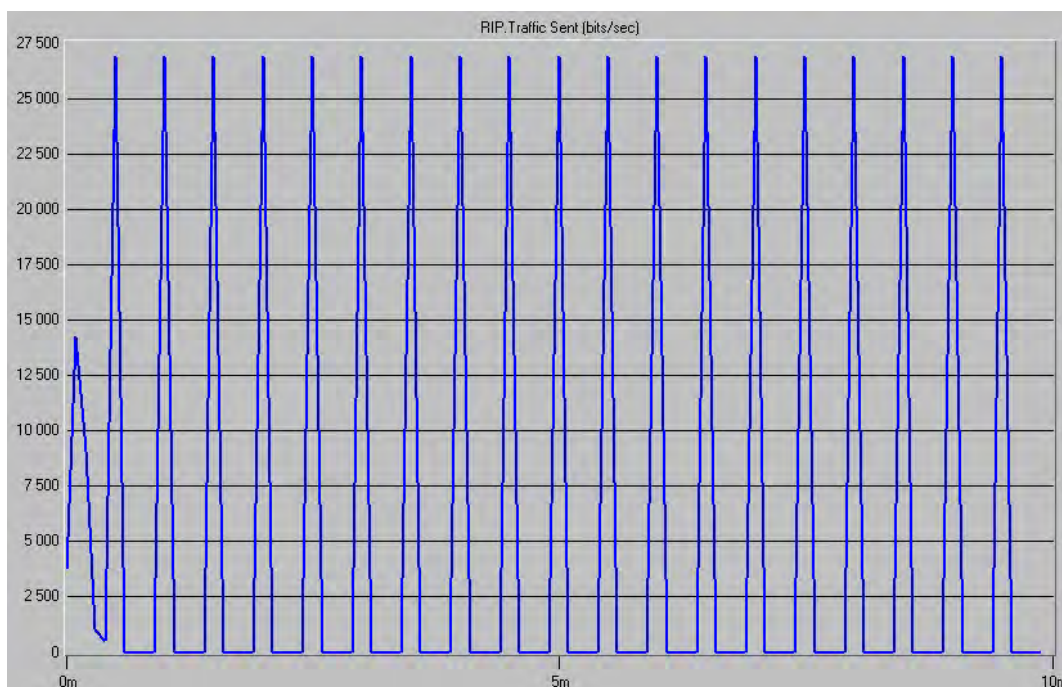
Router name: Campus Network.podsit\_Praha.Praha\_hlavni  
at time: 600,00 seconds

ROUTE TABLE contents:

Dest. Address	Subnet Mask	Next Hop	Interface Name	Metric	Protocol	Insertion
10.10.10.0	255.255.255.0	10.10.10.1	IF0	0	Direct	0,000
10.10.20.0	255.255.255.0	10.10.20.1	IF1	0	Direct	0,000
192.0.5.0	255.255.255.0	192.0.5.2	IF10	0	Direct	0,000
192.0.23.0	255.255.255.0	192.0.23.1	Loopback	0	Direct	0,000
192.0.6.0	255.255.255.0	192.0.5.1	IF10	1	RIP	5,000
192.0.7.0	255.255.255.0	192.0.5.1	IF10	1	RIP	5,000
192.0.8.0	255.255.255.0	192.0.5.1	IF10	1	RIP	5,000
192.0.9.0	255.255.255.0	192.0.5.1	IF10	2	RIP	6,527
192.0.10.0	255.255.255.0	192.0.5.1	IF10	2	RIP	6,527
192.0.11.0	255.255.255.0	192.0.5.1	IF10	2	RIP	6,527
192.0.12.0	255.255.255.0	192.0.5.1	IF10	2	RIP	6,527
192.0.0.0	255.255.255.0	192.0.5.1	IF10	4	RIP	12,389
192.0.1.0	255.255.255.0	192.0.5.1	IF10	3	RIP	12,389
192.0.2.0	255.255.255.0	192.0.5.1	IF10	4	RIP	12,389
192.0.3.0	255.255.255.0	192.0.5.1	IF10	4	RIP	12,389
192.0.4.0	255.255.255.0	192.0.5.1	IF10	4	RIP	12,389
192.0.13.0	255.255.255.0	192.0.5.1	IF10	3	RIP	12,389
192.0.14.0	255.255.255.0	192.0.5.1	IF10	3	RIP	12,389
192.0.15.0	255.255.255.0	192.0.5.1	IF10	3	RIP	12,389
192.0.16.0	255.255.255.0	192.0.5.1	IF10	4	RIP	12,389
192.0.17.0	255.255.255.0	192.0.5.1	IF10	4	RIP	12,389
192.0.18.0	255.255.255.0	192.0.5.1	IF10	3	RIP	12,389
192.0.24.0	255.255.255.0	192.0.5.1	IF10	5	RIP	12,389
192.0.19.0	255.255.255.0	192.0.5.1	IF10	5	RIP	20,085
192.0.20.0	255.255.255.0	192.0.5.1	IF10	5	RIP	20,085
192.0.21.0	255.255.255.0	192.0.5.1	IF10	5	RIP	20,085
192.0.22.0	255.255.255.0	192.0.5.1	IF10	5	RIP	20,085
192.0.25.0	255.255.255.0	192.0.5.1	IF10	6	RIP	20,085
172.16.0.0	255.255.0.0	192.0.5.1	IF10	5	RIP	12,389
150.10.0.0	255.255.0.0	192.0.5.1	IF10	6	RIP	20,085

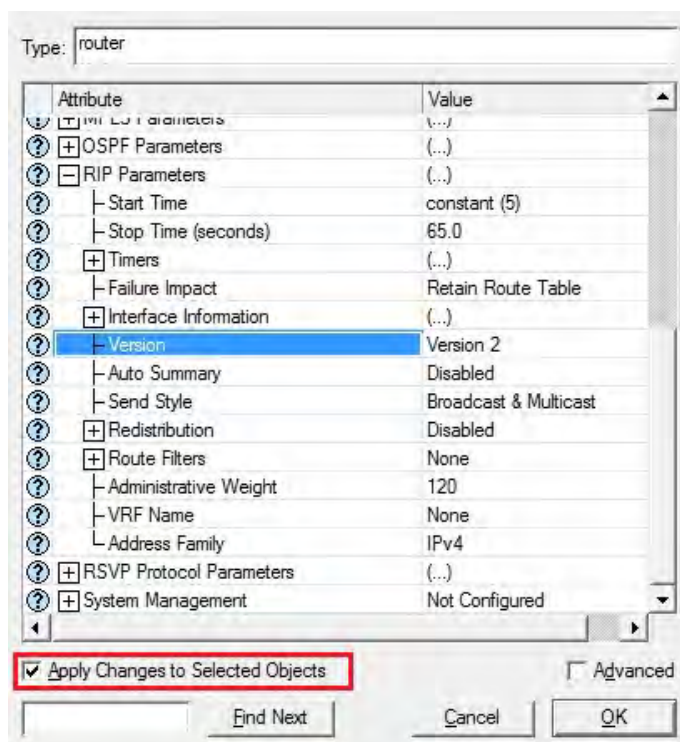
Obr. 9.9: Směrovací tabulka pro směrovač Praha\_hlavni.

19. Po skončení simulace se rovněž zpřístupnila statistika, kterou si můžete zobrazit kliknutím pravého tlačítka na plochu a výběrem *View Results* a v nově otevřeném okně zaškrtnete statistiku *RIP*. Z grafu (Obr. 9.10) je patrné zasílání periodických aktualizací v intervalu 30 sekund.



Obr. 9.10: Statistika celkového RIP provozu v síti v bitech/s.

20. Duplikujte vytvořený scénář (*Scenarios/Duplicate Scenario*). Pro nový scénář nastavte jméno „RIPv2“. Pro přepínání mezi jednotlivými scénáři lze využít položku menu *Scenarios/Switch To Scenario* a vybrat požadovaný scénář.
21. V nově vytvořeném scénáři „RIPv2“ nastavíte na všech směrovačích podporu směrovacího protokolu RIP verze 2. Označte všech 9 směrovačů (pomocí Ctrl a kliknutím levého tlačítka myši) a po kliknutí pravým tlačítkem na jeden ze směrovačů vyberte *Edit Attributes*. Rozklikněte položku *RIP Parameters*. Položku *Version* nastavte na *Version 2*, *Auto Summary* na *Disabled* a *Send Style* na *Broadcast & Multicast*. Důležitě je před vlastním potvrzením zatrhnout červeně označené políčko na obrázku 9.11 *Apply Changes to Selected Objects*, čímž potvrdíte, že chcete nastavené změny aplikovat na všechny označené směrovače. Po potvrzení kliknutím na tlačítko **OK** by se v textové oblasti ve spodní části hlavního okna měla vyspat hláška „9 objects changed“.




Obr. 9.11: Nastavení parametrů pro RIPv2.

22. Postup z předchozího bodu aplikujte i na směrovače uvnitř jednotlivých podsítí. Na směrovače uvnitř podsítě nelze uplatnit hromadné nastavení, proto nastavte zbývající 3 směrovače podle obrázku 9.11 samostatně.

23. Přenastavte masky sítí u rozhraní IF0 a IF1 na směrovači „Praha\_hlavni“ uvnitř „podsit\_Praha“ na hodnotu 255.255.255.252, viz Obr. 9.12.

Attribute	Value
IP Processing Information	(...)
IP Routing Parameters	(...)
Router ID	Auto Assigned
Autonomous System Number	Auto Assigned
Interface Information	(...)
rows	12
row 0	IF0,Active,10.10.10.1,255.255.255.252,Not Use...
row 1	IF1,Active,10.10.20.1,255.255.255.252,Not Use...
row 2	IF2,Active,Auto Assigned,Auto Assigned,Not Us...
row 3	IF3,Active,Auto Assigned,Auto Assigned,Not Us...
row 4	IF4,Active,Auto Assigned,Auto Assigned,Not Us...
row 5	IF5,Active,Auto Assigned,Auto Assigned,Not Us...
row 6	IF6,Active,Auto Assigned,Auto Assigned,Not Us...

Obr. 9.12: Změna nastavení masek u směrovače Praha\_hlavni.

24. Opět spusťte simulaci kliknutím na ikonu  (Run). Veškeré nastavení ponechejte a klikněte na tlačítko **Run** pro zahájení simulace. Po dokončení simulace si můžete shodným způsobem jako u minulého scénáře projít směrovací tabulky i soubor s vypsáním IP adresami, kde si můžete všimnout změny masek u nastavených *classless* adres.

## 9.2.2 Doplnující otázky a úkoly<sup>25</sup>

- 1) Bod 23, ve kterém jste nastavovali nové masky sítí, realizujte i pro scénář „RIP“ a porovnejte změny ve směrovacích tabulkách a stručně zhodnoťte problémy, které by mohli nastat při použití beztrždního adresování u první verze protokolu RIP. Pro vyhodnocení tohoto úkolu použijte směrovací tabulky jiného směrovače než toho uvnitř podsítě Praha.
- 2) U scénáře „RIP“ se vám v okně *Log Browser* mimo směrovacích tabulek objevila i chybová hláška, která říká, že jeden z komponentů „100BaseT\_LAN“ zahazuje UDP datagramy s cílovým portem 520. Pokuste se vysvětlit, proč tomu tak je u scénáře „RIP“ a u scénáře „RIPv2“ již ne.
- 3) Program IT Guru přiřazuje adresní prostor nevhodně (každému

<sup>25</sup> Odpovědi na otázky si poznamenejte (zapamatujte) a na konci cvičení je přednesete vyučujícímu spolu s otázkami z dalších úkolů.

dvoubodovému spoji je přidělena adresa s maskou 255.255.255.0). Určete, jaký adresní prostor je potřeba k návrhu dané topologie při použití směrovacího protokolu RIPv2 a beztřídního adresování? Uvažujte případ, že v každé simulované LAN síti (prvek 100BaseT\_LAN) je 10 PC a 1 server.

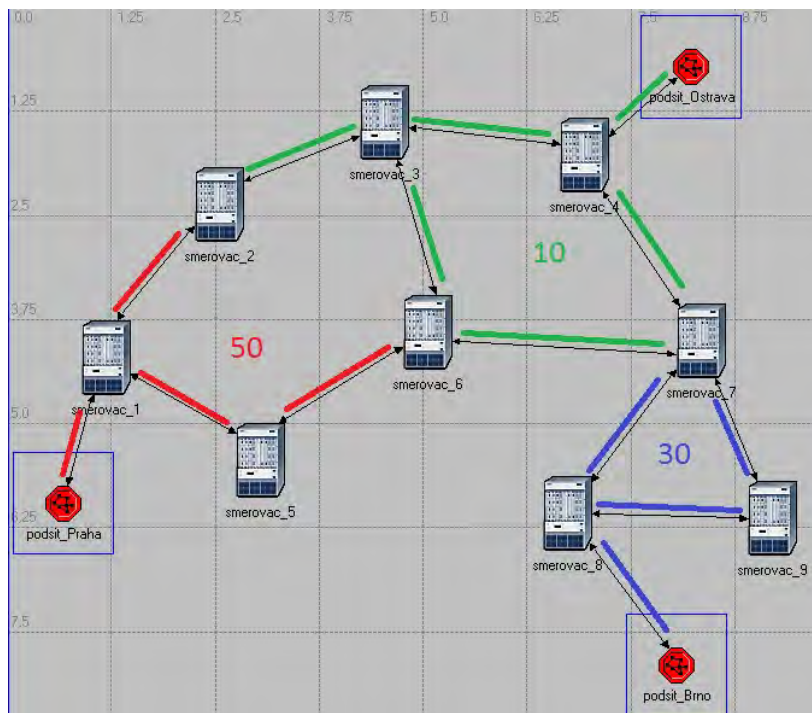
- 4) Do jakých skupin a tříd adres patří vámi přiřazované adresy pro jednotlivé podsítě?
- 5) Zobrazte si statistiku RIP provozu v síti kliknutím pravého tlačítka na plochu a výběrem *View Results*. V okně *View Results* vyberte statistiku *RIP/Traffic Sent* a upřesněte parametry zobrazení grafu na *Overlaid Statistics* a *All Scenarios*. Graf si zobrazíte kliknutím na ikonu **Show**. V zobrazeném grafu můžete pozorovat zvýšenou zátěž u jednoho ze scénářů. U kterého a proč tomu tak je?

## 9.3 Úkol 2 – rozšíření o nové scénáře s OSPF

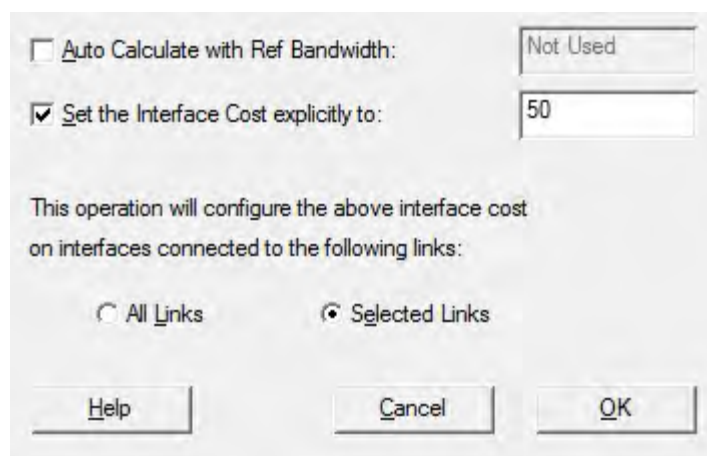
V tomto doplňujícím úkolu budete konfigurovat nové scénáře, ve kterých ke směrování využijete směrovací protokol OSPF. Vytvoříte 2 nové scénáře. V prvním scénáři budou všechny směrovače nastaveny do stejné oblasti, v druhém scénáři topologii rozdělíte na 3 oblasti a budete pozorovat rozdíly v chování sítě. Stejně tak se zaměříte i na rozdíly mezi oběma simulovanými protokoly RIP a OSPF.

### 9.3.1 Postup

1. Duplikujte scénář „RIP“ (*Scenarios/Duplicate Scenario*) a pojmenujte ho „OSPF\_bez\_oblasti“. Pro přepínání mezi jednotlivými scénáři lze využít položku menu *Scenarios/Switch To Scenario* a vybrat požadovaný scénář.
2. V novém scénáři „OSPF\_bez\_oblasti“ nastavíte různé metriky pro jednotlivé spoje, podle obrázku 9.13. Nejprve si označte červeně označené spoje (Ctrl + levé kliknutí myši) a poté vyberte z menu položku *Protocols/OSPF/Configure Interface Cost...*, v následujícím okně zadejte hodnotu 50 a zatrhněte políčko *Selected Links*, viz Obr. 9.14.



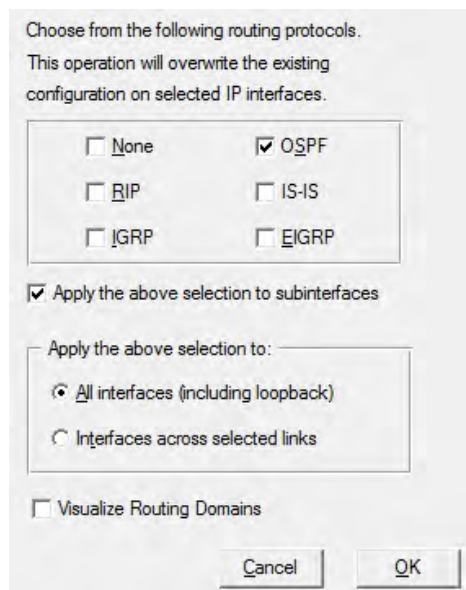
Obr. 9.13: Metriky jednotlivých spojů.



Obr. 9.14: Nastavení metriky pro vybrané spoje.

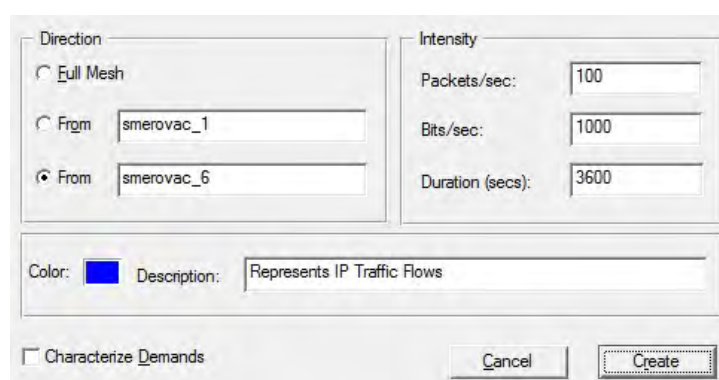
3. Postup z předchozího bodu zopakujte i pro zelené a modré spoje z obrázku 9.13. Pro zeleně označené spoje zadejte hodnotu metriky 10 a pro modře označené spoje zadejte hodnotu 30.
4. Vyberte z menu položku *Protocols/IP/Routing/Configure Routing Protocols*. V nově otevřeném okně zatrhněte možnost *OSPF* a *All Interfaces*, viz Obr. 9.15.





Obr. 9.15: Nastavení směrovacího protokolu OSPF.


5. V tomto kroku nastavíte IP provoz mezi směrovači 1 a 6. Označte proto směrovače „*smerovac\_1*“ a „*smerovac\_6*“. K označení dvou a více prvků opět využijete klávesu Ctrl. Po označení vyberte položku menu *Protocols/IP/Demands/Create Traffic Demands...* V následujícím okně vyberete provoz ze „*smerovac\_6*“, viz obrázek 9.16 a potvrdíte kliknutím na **Create**. Nakonfigurovaný síťový provoz bude poté ve scénáři označen přímou modrou tečkovanou čarou, viz 9.20.

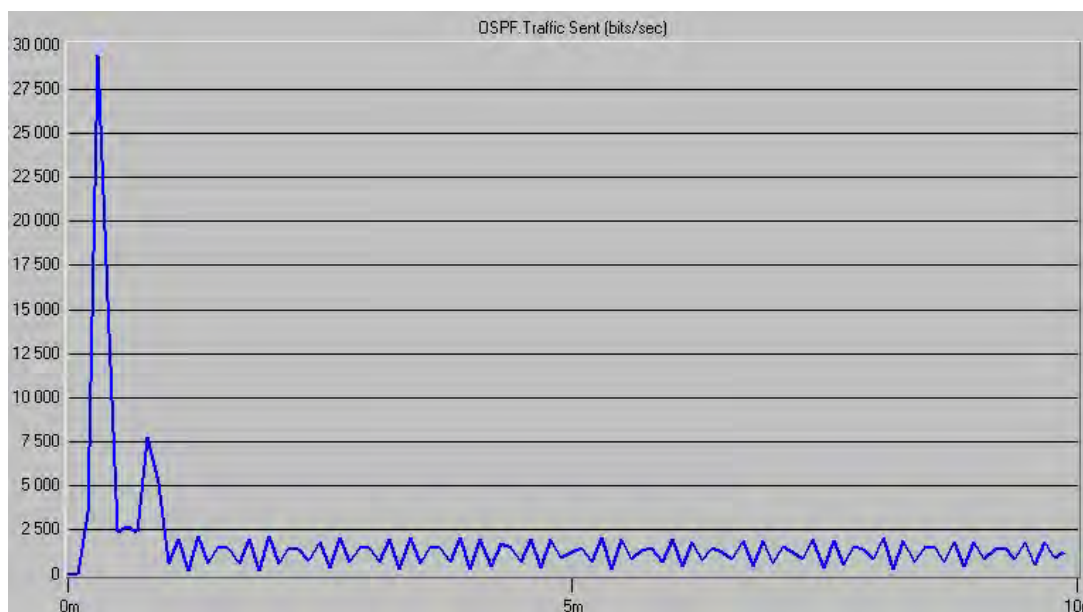


Obr. 9.16: Konfigurace IP provozu mezi směrovači 1 a 6.

6. Před spuštěním simulace vyberete statistiku zobrazující OSPF provoz během simulace. Statistiku vyberete kliknutím pravého tlačítka myši na plochu a výběrem *Choose Individual Statistics*. V nově otevřeném okně *Choose Results* vyberete

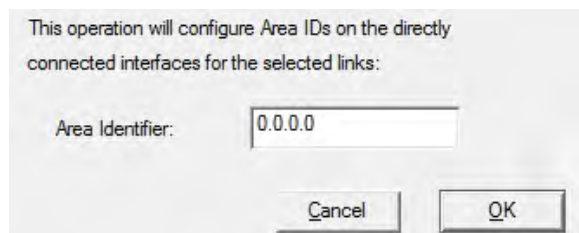
v *Global Statistics/OSPF* položku *Traffic Sent (bits/sec)*. Označte pouze statistiku OSPF provozu, případné další přednastavené statistiky odznačte.

7. Stisknutím ikony  (Run) opět vstoupíte do konfiguračního okna simulace, kde v záložce *Common* ponecháte nastavené hodnoty z předešlé simulace. V záložce *Global Attributes* nastavte položku *IP Dynamic Routing Protocol* na *OSPF* a u *OSPF Sim Efficiency* vyberte *Disabled*. Touto možností zajistíte funkčnost směrovacího protokolu během celé simulace, nejen na přednastavený čas. Pro spuštění simulace stiskněte tlačítko **Run**.
8. Po skončení simulace se zpřístupnila statistika, kterou si můžete zobrazit kliknutím pravého tlačítka na plochu a výběrem *View Results* a v nově otevřeném okně zaškrtnete statistiku *OSPF/Traffic Sent*. (Obr. 9.17)



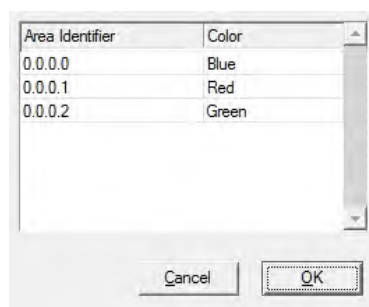
Obr. 9.17: Statistika OSPF provozu v topologii bez oblastí v bitech/s.

9. Duplikujte scénář „OSPF\_bez\_oblasti“ (*Scenarios/Duplicate Scenario*) a pojmenujte ho „OSPF\_oblasti“.
10. V novém scénáři rozdělíte topologii na 3 oblasti. Oblasti budou tvořit stejné spoje jako u přiřazování metrik. Nejprve tedy vyberte všechny zeleně označené spoje a z menu vyberte položku *Protocols/OSPF/Configure Areas...*, v následujícím okně zadejte identifikátor oblasti 0.0.0.0, viz Obr. 9.18.



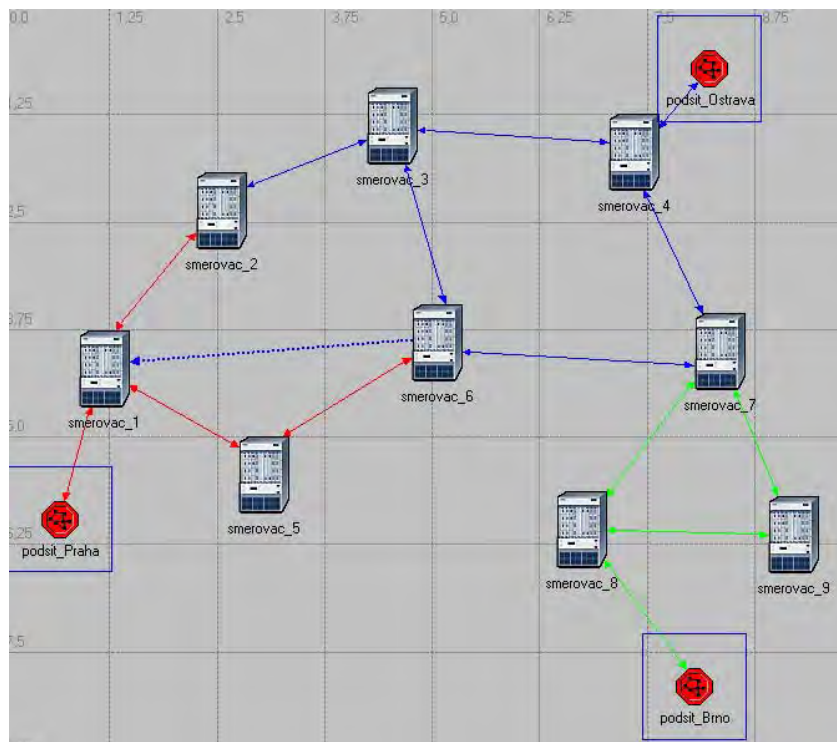
Obr. 9.18: Konfigurace jednotlivých oblastí.

11. Postup z předchozího bodu zopakujte i pro červené a modré spoje z obrázku 9.14. Pro červeně označené spoje zadejte identifikátor oblasti 0.0.0.1 a pro modře označené spoje 0.0.0.2.
12. Po nastavení jednotlivých oblastí můžete pro názornost využít možnosti vizualizace oblastí výběrem položky z menu *Protocols/OSPF/Visualize Areas...* (Obr. 9.19).




Obr. 9.19: Vizualizace oblastí.





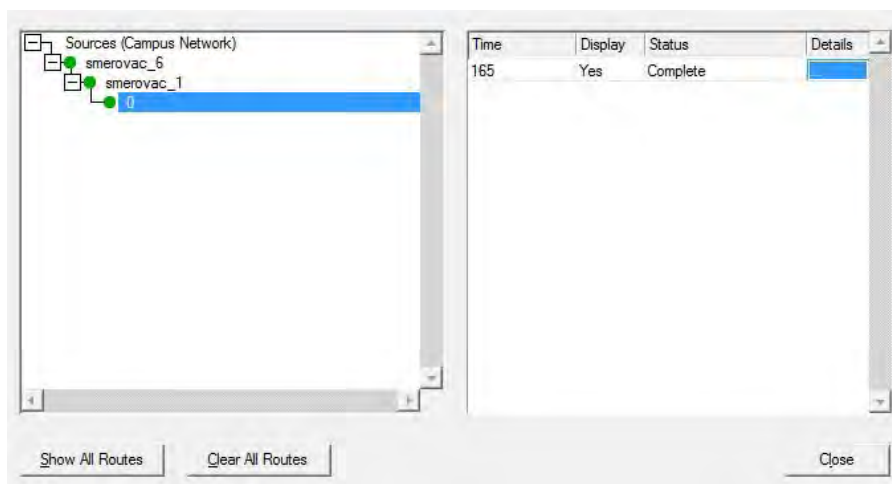
Obr. 9.20: Topologie s nastavenými a vizualizovanými oblastmi.

13. Stisknutím ikony  (Run) opět vstoupíte do okna nastavení parametrů simulace, kde ponecháte všechny hodnoty a stisknutím tlačítka **Run** spustíte simulaci.

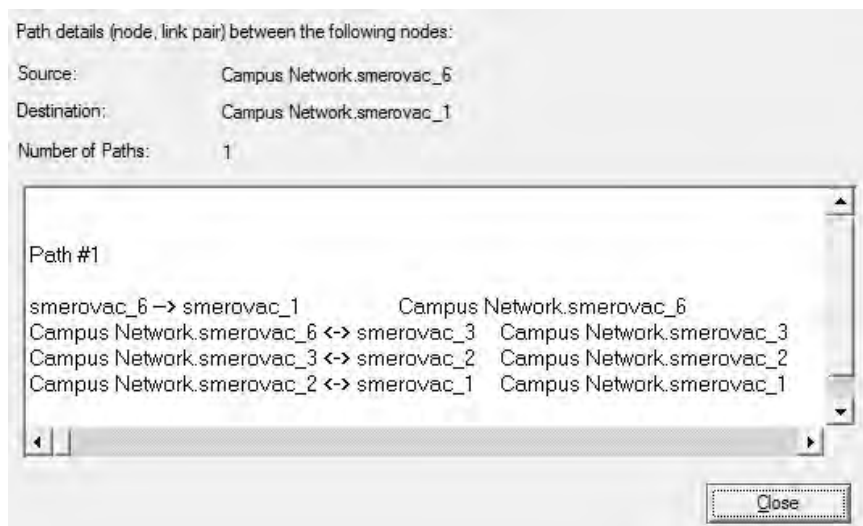
### 9.3.2 Doplnující otázky a úkoly

- 1) Zobrazte si směrovací tabulky u obou OSPF scénářů a porovnejte je mezi sebou. Směrovací tabulky si zobrazíte kliknutím pravým tlačítkem myši na plochu a výběrem možnosti *Open Simulation Log*. V okně *Log Browser* již můžete vybrat jednu ze směrovacích tabulek kliknutím do oblasti *Message*. Zobrazte si směrovací tabulku pro směrovač, který přísluší pouze do jedné OSPF oblasti (například směrovač „Brno\_hlavni“) shodný pro oba OSPF scénáře a porovnejte. Směrovací tabulky OSPF porovnejte i s tabulkami RIP protokolu. Zaměřte se zejména na rozdíly ve směrovacích tabulkách.
- 2) Který protokol potřebuje delší čas pro sestavení směrovacích tabulek? Uveďte časy zjištěné ze směrovacích tabulek. Zamyslete se nad tím, proč je mezi směrovacími protokoly takový rozdíl.

- 3) Zobrazte si směrovací tabulku pro „směrovač\_6“. Ve směrovací tabulce směrovače\_6 si můžete všimnout vlastnosti směrovacího protokolu OSPF uchovávat v tabulce více cest do stejného cíle se stejnou metrikou, čehož protokol může využívat k rozložení zátěže v síti.
- 4) Zobrazte si statistiku OSPF provozu v síti kliknutím pravého tlačítka na plochu a výběrem *View Results*. V okně *View Results* vyberte statistiku *OSPF/Traffic Sent* a upřesněte parametry zobrazení grafu na *Overlaid Statistics* a *All Scenarios*. Graf si zobrazíte kliknutím na ikonu **Show**. V zobrazeném grafu můžete pozorovat zvýšenou zátěž u jednoho ze scénářů. U kterého a proč tomu tak je?
- 5) Porovnejte statistiku OSPF provozu v síti s provozem u RIP protokolu. Porovnejte vhodnost protokolů pro sítě s častými změnami v topologii.
- 6) Zobrazte si nakonfigurovaný provoz mezi směrovači 1 a 6. Vstupte do menu *Protocols/IP/Demands/Display Routes for Configured Demands...* V nově otevřeném okně (Obr. 9.21) vyberte definovaný provoz a klikněte na položku *Details* pro zobrazení detailů o provozu. Otevře se vám okno *Path Details*, v kterém zjistíte cestu mezi jednotlivými směrovači. Na obrázku 9.22 je znázorněn výpis pro scénář „OSPF\_bez\_oblasti“ bez nakonfigurovaných oblastí. Zobrazte si výpis i pro scénář OSPF s oblastmi a cestu porovnejte.



Obr. 9.21: Zobrazení nastaveného IP provozu mezi směrovači.



Obr. 9.22: Výpis cesty mezi směrovači 1 a 6 pro scénář OSPF\_bez\_oblasti.

## 9.4 Úkol 3 – nastavení výpadku linky

V tomto doplňujícím úkolu bude simulován výpadek linky jak pro scénář OSPF bez oblastí, tak pro scénář OSPF s oblastmi.

### 9.4.1 Postup

1. Duplikujte scénář „OSPF\_bez\_oblasti“ (*Scenarios/Duplicate Scenario*) a pojmenujte ho „OSPF\_bez\_oblasti\_vypadek“. Pro přepínání mezi jednotlivými scénáři lze využít položku menu *Scenarios/Switch To Scenario* a vybrat požadovaný scénář.
2. V nově vytvořeném scénáři vložte na plochu z okna *Object Palette* prvek „Failure Recovery“ a pojmenujte ho „vypadek/obnova“.
3. Daný prvek nastavíte podle obrázku 9.23, tak aby v čase 200 sekund nastal výpadek linky mezi směrovači 1 a 2. V čase 500 sekund naopak nastane obnova dané linky.

Type: Utilities

Attribute	Value
? name	vypadek/obnova
? model	Failure Recovery
? Failure/Recovery Modeling	Enabled
? Link Failure/Recovery Specification	(...)
? rows	2
row 0	
? Name	Campus Network.smerovac_2 <-> smerovac_1
? Time	200
? Status	Fail
row 1	
? Name	Campus Network.smerovac_2 <-> smerovac_1
? Time	500
? Status	Recover
? Link Failure/Recovery Specification File	NOT_USED
? Node Failure Mode	Node only
? Node Failure/Recovery Specification	No Failure/Recovery

Obr. 9.23: Nastavení výpadku a obnovení spoje.

- Po nastavení výpadku a obnovení linky nastavíte směrovač uvnitř podsítě „podsit\_Brno“ tak, aby se vygenerovala nová směrovací tabulka v různých časech simulace. Vstoupíte proto do konfigurace směrovače „Brno\_hlavni“ a nastavíte hodnotu *IP Routing Parameters/Routing Table Export/Export Times Specification* podle obrázku 9.24. Směrovací tabulka se tak bude generovat v časech 150 s, 350 s, a na konci simulace.

Attribute	Value
IP Processing Information	(...)
IP Routing Parameters	(...)
Router ID	Auto Assigned
Autonomous System Number	Auto Assigned
Interface Information	(...)
Loopback Interfaces	(...)
Default Route	Auto Assigned
Static Routing Table	None
Load Balancing Options	Destination-Based
Routing Table Export	(...)
Status	Enabled
Export Time(s) Specification	(...)
rows	3
row 0	
Time	150
row 1	
Time	350
row 2	
Time	End of Simulation

Obr. 9.24: Nastavení exportu směrovací tabulky v různých časech.

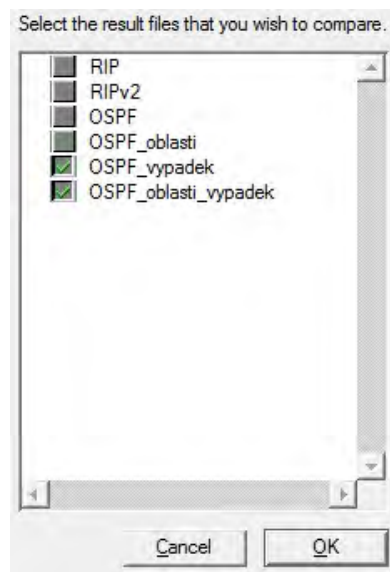
5. V předchozích bodech tohoto úkolu jste si připravili scénář pro výpadek a obnovu linky pro scénář „OSPF\_bez\_oblasti“. Tento postup (bod 1 až 4) zopakujte pro scénář „OSPF\_oblasti“. V prvním kroku tak duplikujete scénář „OSPF\_oblasti“ a nový scénář pojmenujete „OSPF\_oblasti\_vypadek“. Kroky 2 až 4 jsou shodné s předchozím scénářem.
6. Po nastavení obou nových scénářů spustíte simulaci obou scénářů, k čemuž můžete využít položku menu *Scenarios/Manage Scenarios...* a v nově otevřeném okně u nově vytvořených scénářů vybrat u položky *Results* <collect> respektive <recollect>, viz Obr. 9.25. Simulaci zahájíte kliknutím na ikonu **OK**.

Project Name: RIP_OSPF					
#	Scenario Name	Saved	Results	Sim Duration	Time Units
1	RIP	saved	out of date	10	minute(s)
2	RIPv2	saved	out of date	10	minute(s)
3	OSPF_bez_oblasti	saved	out of date	10	minute(s)
4	OSPF_oblasti	saved	out of date	10	minute(s)
5	OSPF_bez_oblasti_vypadek	saved	<recollect>	10	minute(s)
6	OSPF_oblasti_vypadek	saved	<collect>	10	minute(s)

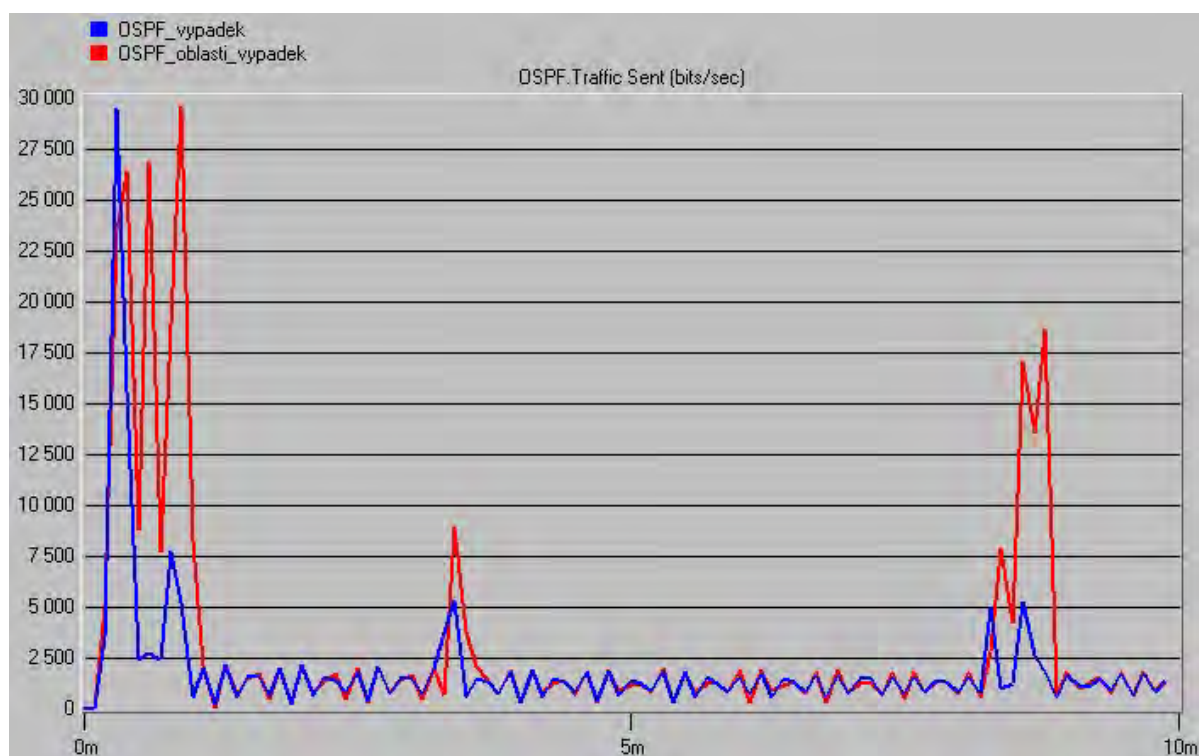
Obr. 9.25: Simulování scénářů pomocí Manage Scenarios.

### 9.4.2 Doplňující otázky a úkoly

- 1) Znáмым postupem (kliknutím pravého tlačítka myši na plochu a výběrem položky *Open Simulation Log*) si zobrazte směrovací tabulky pro směrovač „Brno\_hlavni“ a porovnejte tabulky v různých časech simulace (po výpadku a obnově spoje) pro oba nově vytvořené scénáře.
- 2) Ze směrovacích tabulek vyvoďte závěr, jak dlouho trvá směrovacímu protokolu reakce na výpadek či obnovu linky v dané topologii a porovnejte se známou rychlostí u směrovacího protokolu RIP.
- 3) Zobrazte si statistiku OSPF provozu v síti kliknutím pravého tlačítka na plochu a výběrem *View Results*. V okně *View Results* vyberte statistiku *Global Statistics/OSPF/Traffic Sent* a upřesněte parametry zobrazení grafu na *Overlaid Statistics* a *Select Scenarios*. Graf si zobrazíte kliknutím na ikonu **Show** a při dotazu programu na výběr scénářů vyberete „OSPF\_bez\_oblasti\_vypadek“ a „OSPF\_oblasti\_vypadek“, viz Obr. 9.26. Na výsledném grafu (Obr. 9.27) si můžete všimnout zvýšeného provozu u topologie rozdělené na oblasti při výpadku a obnově linky oproti topologii bez oblastí. V čem je tedy výhoda rozdělení sítě na jednotlivé oblasti? Své tvrzení můžete podpořit nakonfigurováním statistiky provozu OSPF na jednotlivých směrovačích. Postup je shodný, jako při výběru globální statistiky, pouze nekliknete na plochu pravým tlačítkem myši, ale na požadovaný objekt, na kterém chcete nastavit statistiku a vyberete možnost *Choose Individual Statistics*.



Obr. 9.26: Výběr požadovaných scénářů u možnosti Select Scenarios.



Obr. 9.27: Celkový OSPF provoz v síti s oblastmi i bez oblastí s výpadkem linky v bitech/s.

## 10 TECHNOLOGIE ATM A FRAME RELAY

Tato laboratorní úloha je zaměřena na přenosové technologie pro sítě typu *Wide Area Network* (WAN), což jsou sítě pro přenos dat na dlouhé vzdálenosti s dosahem stovky až tisíce kilometrů. V úloze se seznámíte se základními vlastnostmi sítí ATM (*Asynchronous Transfer Mode*) a Frame Relay. ATM byla navržena pro přenos hlasu a dat a pro přenos využívá buňky s pevnou délkou o velikosti 53 bajtů (5 bajtů záhlaví, 48 bajtů data). Technologie Frame Relay se používá zejména v sítích WAN a využívá přepínání paketů [1]. Technologie je založena především na sestavení trvalých virtuálních okruhů mezi dvěma síťovými zařízeními.

### 10.1 Úkol 1 - ATM

V prvním úkolu této úlohy vytvoříte topologii pro simulování technologie ATM. Pro technologii ATM je charakteristické používání tříd služeb pro rozlišení zacházení s daty od různých aplikací. Aplikace pro přenos hlasu mají odlišné nároky na přenosové parametry sítě než například FTP provoz. Proto v části úlohy věnované ATM budete třídit provoz do jednotlivých tříd služeb a přiřazovat adaptační protokoly tak, abyste se seznámili se základními vlastnostmi ATM protokolu.

#### 10.1.1 Popis vytvoření programu

1. Spustíte program OPNET IT Guru Academic Edition.
2. Z menu programu vyberte položku **File/New...** (Ctrl + N) a v rolovací nabídce ponechejte „Project“ a potvrďte tlačítkem **OK**.
3. V následujícím okně zadejte jméno projektu a scénáře. Jméno projektu zvolte například „ATM\_FR“ (*Project Name*) a jméno scénáře „ATM\_CBR\_ABR\_0“<sup>26</sup> (*Scenario Name*).
4. Následně nechte vybranou položku „Create Empty Scenario“ a klikněte na **Next**.

---

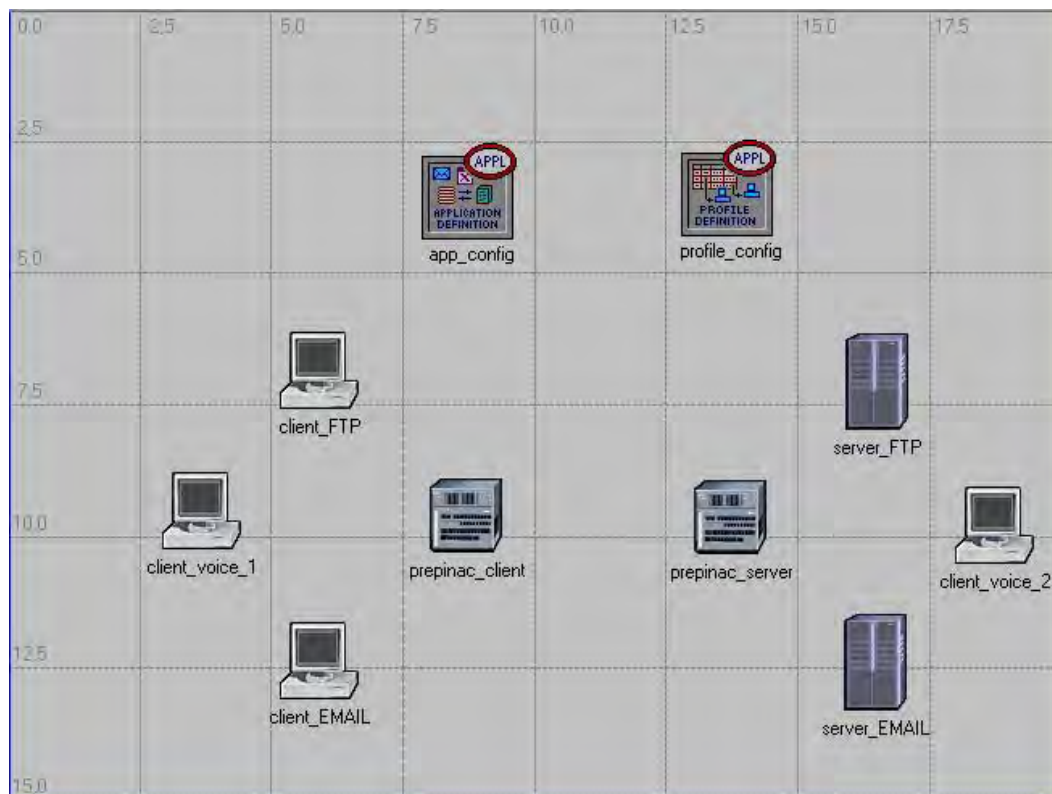
<sup>26</sup> V daném názvu scénáře první třída služeb vždy bude označovat nastavenou třídu služeb pro hlasovou aplikaci. Druhá položka značí přiřazenou třídu služeb datovým aplikacím a číslo vyjadřuje nastavený provoz na pozadí. Pro scénář „ATM\_CBR\_ABR\_0“ tedy bude nastavena třída služeb CBR pro hlasovou aplikaci a třída služeb ABR pro datové aplikace. Dále prozatím bude v síti nastaven nulový provoz na pozadí.



5. Při výběru rozlohy označte položku „Campus“ a ponechejte zaškrtnuté „Use Metric Units“. Klikněte na **Next** a zadejte požadovanou rozlohu 20x15 kilometry.
6. V následujícím kroku máte na výběr několik technologií. Zatrhněte „atm\_advanced“, „ethernet“, „frame relay“ a „routers“ a klikněte na **Next**. Poté potvrďte volbou **OK** požadované nastavení, které si ještě jednou můžete zkontrolovat v přehledu.<sup>27</sup>
7. Vložte na plochu postupně tyto komponenty z okna *Object Palette*:
  - I. Application Config
  - II. Profile Config
  - III. 4x atm\_uni\_client\_adv
  - IV. 2x atm\_uni\_server\_adv
  - V. 2x atm8\_crossconn\_adv
8. Komponenty rozmístěte na plochu a pojmenujte podle Obr. 10.1. Zároveň se jménem prvku budete nastavovat adresy jednotlivých prvků. Adresy a jména prvků budete nastavovat na všech klientech a serverech. V následujícím textu bude popsán postup pro nastavení jména a adresy na prvku „client\_FTP“. Kliknete na daného klienta pravým tlačítkem a vyberete položku *Edit Attributes*. U všech prvků zadáte stejnou adresu, jako je název daného prvku. Pro FTP klienta tedy zadáte jméno (položka *name*) i adresu (položka *Client Address*, případně *Server Address* pro server) *client\_FTP*. (Obr. 10.2) Daný postup zopakujte pro zbylé 3 klienty a 2 servery.

---

<sup>27</sup> Stejně jako při práci s jakýmkoliv jiným programem doporučuji práci průběžně ukládat (Ctrl + S). Při prvním uložení se program IT Guru dotáže, jestli opravdu chceme uložit projekt pod námi již definovaným názvem. Uložení je vhodné provádět vždy po změně či nastavení nějaké z komponent tak, aby se nastavené parametry zpřístupnili i pro nastavování dalších komponent.

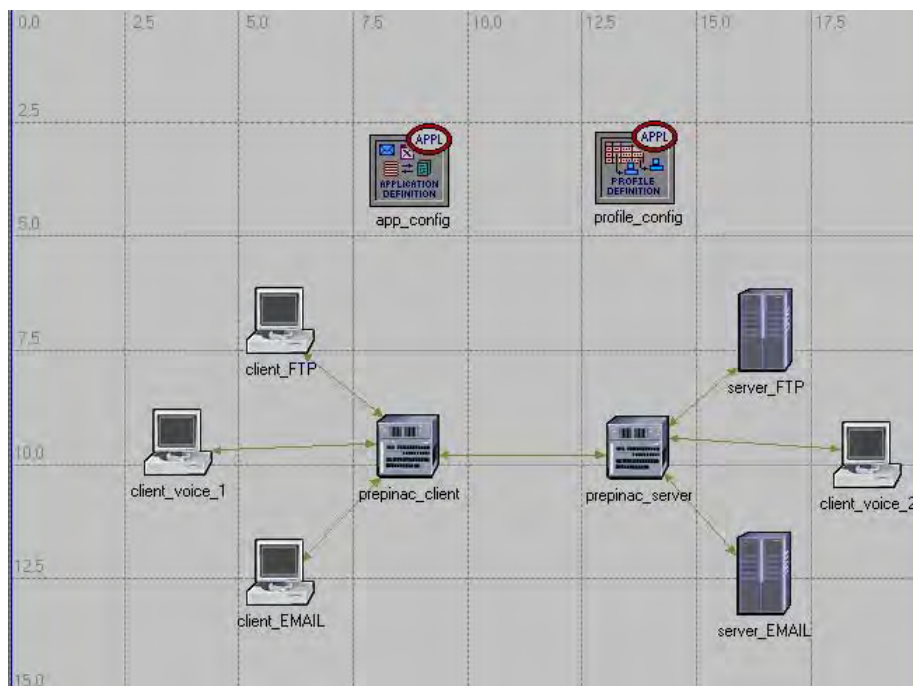


Obr. 10.1: Základní topologie bez propojení.

Attribute	Value
? name	client_FTP
? model	atm_uni_client_adv
? + ATM Application Parameters	UBR Only
? + ATM Parameters	(...)
? + Application: ACE Tier Configuration	Unspecified
? Application: Destination Preferences	None
? + Application: Multicasting Specification	None
? + Application: RSVP Parameters	None
? Application: Segment Size	64,000
? + Application: Source Preferences	None
? + Application: Supported Profiles	None
? Application: Supported Services	None
? + Application: Transport Protocol	AAL5
? + CPU Background Utilization	None
? + CPU Resource Parameters	Single Processor
? Client Address	client_FTP
? + SIP UAC Parameters	(...)
? + Server: Advanced Server Configuration	Sun Ultra 10 333 MHz
? Server: Modeling Method	Simple CPU

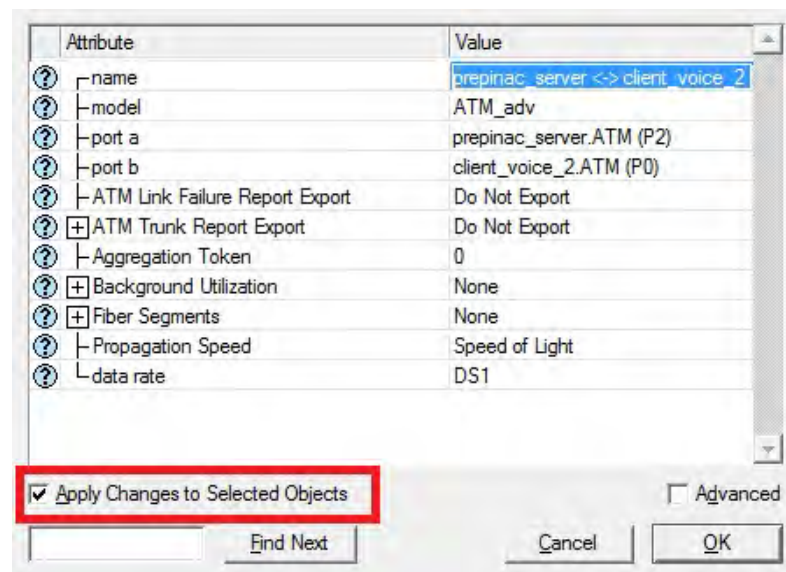
Obr. 10.2: Nastavení názvu a adresy pro klienta FTP.

9. Po rozmístění a pojmenování jednotlivých prvků přistoupíte k propojení topologie pomocí obousměrné linky „ATM\_adv“, viz Obr. 10.3. Prvky propojíte prostým označením spoje „ATM\_adv“ v okně *Object Palette* a pak kliknutím na požadované prvky, které chcete propojit.



Obr. 10.3: Propojení topologie spojem ATM\_adv.

10. Pomocí tlačítka Ctrl a levého kliknutí myši si označte všech 7 vytvořených spojů a vstupte do nastavení parametrů spoje pravým kliknutím myši na spoj a výběrem *Edit Attributes* z kontextového menu. V nově otevřeném okně *Edit Attributes* změňte poslední položku „data rate“ na hodnotu „DSI“, viz Obr. 10.4. Před potvrzením zatrhněte červeně označené políčko na obrázku 10.4 pro nastavení na všech 7 spojích. Správnost nastavení si můžete ověřit výpisem hlášky *7 objects changed* v textové oblasti programu.



Obr. 10.4: Hromadné nastavení linky na přenosovou rychlost DS1.

11. Nyní máte nakonfigurovanou základní topologii a přistoupíte k nastavování jednotlivých komponent. V prvním kroku budete nastavovat komponentu *app\_config*. V této komponentě se definují parametry aplikace. Vstupte do konfiguračního prostředí komponenty kliknutím pravým tlačítkem myši na ikonu a vybráním *Edit Attributes*. V záložce „*Application Definitions*“ nastavte *Rows* na 3. Jednotlivé aplikace pojmenujte „FTP\_app“, EMAIL\_app a VOICE\_app. U aplikace „FTP\_app“ nastavte pole „FTP“ na „Low Load“, viz Obr. 10.5. Podobně u aplikace „EMAIL\_app“ nastavte položku „Email“ na „Low Load“ a pro aplikaci „VOICE\_app“ nastavte položku „Voice“ na hodnotu „PCM Quality Speech“. Nastavení potvrďte tlačítkem **OK**.

Attribute	Value
[-] row 0	
[-] Name	FTP_app
[-] Description	(...)
[-] Custom	Off
[-] Database	Off
[-] Email	Off
[-] Ftp	Low Load
[-] Http	Off
[-] Print	Off
[-] Remote Login	Off
[-] Video Conferencing	Off
[-] Voice	Off
[-] row 1	
[-] Name	EMAIL_app
[+] Description	(...)
[-] row 2	
[-] Name	VOICE_app
[+] Description	(...)

Obr. 10.5: Nastavení aplikací a jejich parametry.

12. V dalším kroku pro nastavené aplikace vytvoříte profily v prvku *Profile Config*. Opět klikněte pravým tlačítkem na komponentu *Profile Config*, vyberte položku „*Edit Attributes*“. V nově otevřeném okně u položky „*Profile Configuration*“ změňte hodnotu „*rows*“ na 3. Budete tedy nastavovat 3 profily, pro každou aplikaci jeden. Jméno prvního profilu nastavte „FTP\_prof“ a nastavte položky *Name*, *Start Time Offset (seconds)*, *Duration (seconds)*, *Repeatability/Inter-repetition Time (seconds)* a *Start Time (seconds)* podle obrázku 10.6. Pro druhý profil zvolte jméno „EMAIL\_prof“ a opět nastavte shodné položky podle obrázku 10.7. U těchto dvou profilů je využité rozložení *constant*. Jméno posledního profilu nastavte na „VOICE\_prof“ a zkontrolujte nastavení podle obrázku 10.8. Nastavení potvrďte kliknutím na tlačítko **OK**.

Attribute	Value
[-] Profile Configuration	(...)
[-] rows	3
[-] row 0	
[-] Profile Name	FTP_prof
[-] Applications	(...)
[-] rows	1
[-] row 0	
[-] Name	FTP_app
[-] Start Time Offset (seconds)	constant (5)
[-] Duration (seconds)	constant (20)
[-] Repeatability	(...)
[-] Inter-repetition Time (sec...	constant (50)
[-] Number of Repetitions	Unlimited
[-] Repetition Pattern	Serial
[-] Operation Mode	Serial (Ordered)
[-] Start Time (seconds)	constant (100)
[-] Duration (seconds)	End of Simulation
[-] Repeatability	(...)
[-] Inter-repetition Time (seconds)	constant (300)
[-] Number of Repetitions	constant (0)
[-] Repetition Pattern	Serial

Obr. 10.6: Nastavení profilu pro aplikaci FTP.

Attribute	Value
[-] Repetition Pattern	Serial
[-] row 1	
[-] Profile Name	EMAIL_prof
[-] Applications	(...)
[-] rows	1
[-] row 0	
[-] Name	EMAIL_app
[-] Start Time Offset (seconds)	constant (5)
[-] Duration (seconds)	constant (50)
[-] Repeatability	(...)
[-] Inter-repetition Time (sec...	constant (100)
[-] Number of Repetitions	Unlimited
[-] Repetition Pattern	Serial
[-] Operation Mode	Serial (Ordered)
[-] Start Time (seconds)	constant (100)
[-] Duration (seconds)	End of Simulation
[-] Repeatability	(...)
[-] Inter-repetition Time (seconds)	constant (300)
[-] Number of Repetitions	constant (0)
[-] Repetition Pattern	Serial
[+] row 2	VOICE_prof.(...),Serial (Ord

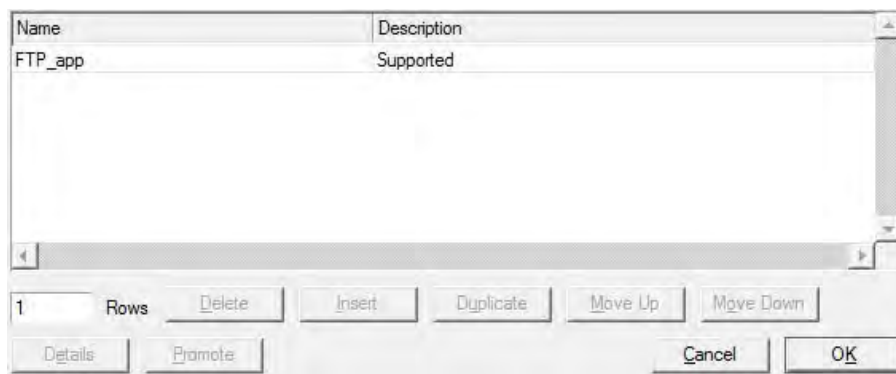
Obr. 10.7: Nastavení profilu pro aplikaci EMAIL.



?	└ Repetition Pattern	Serial
	└ row 1	EMAIL_prof,(...),Serial (Order)
	└ row 2	
?	└ Profile Name	VOICE_prof
?	└ Applications	(...)
?	└ rows	1
	└ row 0	
?	└ Name	VOICE_app
?	└ Start Time Offset (seconds)	uniform (5,10)
?	└ Duration (seconds)	End of Profile
?	└ Repeatability	(...)
?	└ Inter-repetition Time (sec...	exponential (300)
?	└ Number of Repetitions	Unlimited
?	└ Repetition Pattern	Serial
?	└ Operation Mode	Serial (Ordered)
?	└ Start Time (seconds)	uniform (100,110)
?	└ Duration (seconds)	End of Simulation
?	└ Repeatability	(...)
?	└ Inter-repetition Time (seconds)	constant (300)
?	└ Number of Repetitions	constant (0)
?	└ Repetition Pattern	Serial

Obr. 10.8: Nastavení profilu pro aplikaci VOICE.

13. Po nastavení aplikací a profilů musíte ještě zajistit podporu těchto aplikací a profilů na serverech a klientech. Nastavení jednotlivých prvků je popsáno v následujících bodech. V bodu 19 je pak shrnutí nastavení pro všechny klienty a servery. Nejprve nastavíte „server\_FTP“, vstupte proto do nastavení atributů (*Edit Attributes*). V poli *Application: Supported Services* vyberte dříve definovanou aplikaci „FTP\_app“, viz Obr. 10.9. U položky *ATM Application Parameters* vyberte hodnotu „ABR only“ a v položce *ATM Parameters/Queue Configuration* vyberte možnost „ABR Only (Per VC Queue)“ (Obr. 10.10). Tím zajistíme, že FTP server bude pro komunikaci využívat pouze třídu služeb ABR.



Obr. 10.9: Podpora aplikace na serveru (*Supported Services*).

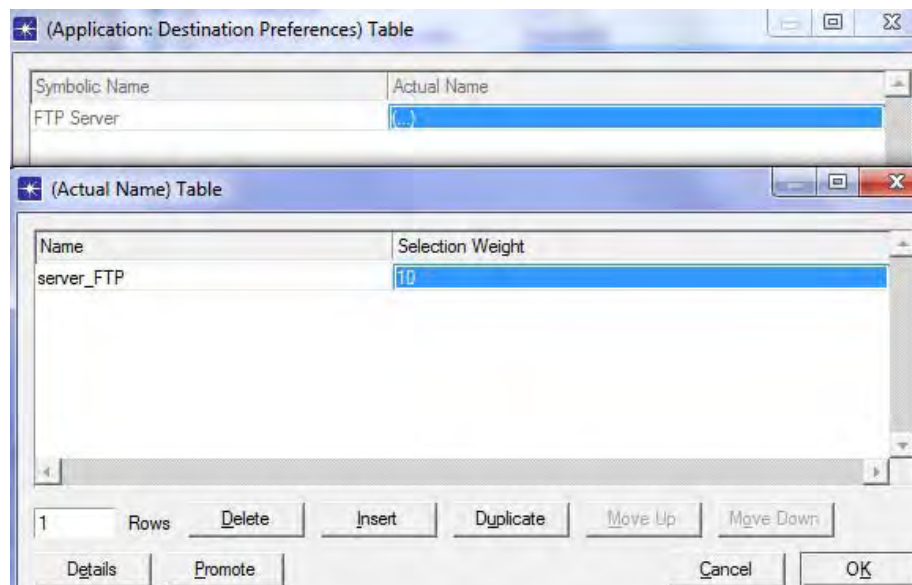
14. Postup z předcházejícího bodu opakujte pro „server\_EMAIL“ s tím rozdílem, že u podporované aplikace vyberete „EMAIL\_app“.

Attribute	Value
name	server_FTP
model	atm_uni_server_adv
ATM Application Parameters	ABR Only
ATM Parameters	(...)
Address	Auto Assigned
Queue Configuration	ABR Only (Per VC Queue)
Per-Port Configuration	(...)
VC Routes Report	Do Not Export

Obr. 10.10: Nastavení třídy služeb ABR na serveru FTP.

15. Po nastavení serverů přistoupíte k nastavení klientů. Nejprve vstupte do konfigurace atributů na prvku „client\_FTP“. V poli *Application: Supported Profiles* nastavte dříve vytvořený profil „FTP\_prof“. Dále je nutné nastavit položku *Application:Destination Preferences*, u které v nově otevřeném okně vyberete u položky *Symbolic Name* položku „FTP Server“ a jméno u pole *Actual Name* nastavte „server\_FTP“. (Obr. 10.11) Dále stejně jako u serveru nastavíte třídu služeb na ABR. Konkrétně tedy nastavíte položku *ATM Application Parameters* na hodnotu „ABR only“ a v položce *ATM Parameters/Queue Configuration* vyberte možnost „ABR Only (Per VC Queue)“, podobně jako na obrázku 10.10.





Obr. 10.11: Nastavení podpory serveru pro klienta FTP.

16. Předchozí bod zopakujete pro nastavení prvku „client\_EMAIL“ s tím rozdílem, že nastavíte „EMAIL\_prof“ u podporovaných profilů a u položky *Application:Destination Preferences* vyberete u položky *Symbolic Name* položku „Email Server“ a jméno u pole *Actual Name* nastavte na „server\_EMAIL“.
17. Nyní zbývá nastavit 2 klienty, pro podporu *voice* aplikace. Vstupte proto do nastavení prvku „client\_voice\_1“. Proved'te následující nastavení:  
*ATM Application Parameters* nastavíte na hodnotu „CBR only“,  
*ATM Parameters/Queue Configuration* nastavte na „CBR Only“,  
*Application: Supported Profiles* nastavte profil „VOICE\_prof“,  
*Application: Supported Services* nastavte aplikaci „VOICE\_app“,  
*Application: Transport Protocol/Voice Transport* nastavte adaptační protokol AAL2<sup>28</sup>  
*Application: Destination Preferences/Symbolic Name* na hodnotu „Voice Destination“ a u pole *Actual Name* vyberete „client\_voice\_2“.
18. Stejné nastavení z bodu 17 provedete i pro klienta „client\_voice\_2“, pouze u posledního bodu vyberete u položky *Actual Name* jméno „client\_voice\_1“.
19. Přehled všech nastavení pro klienty a servery:

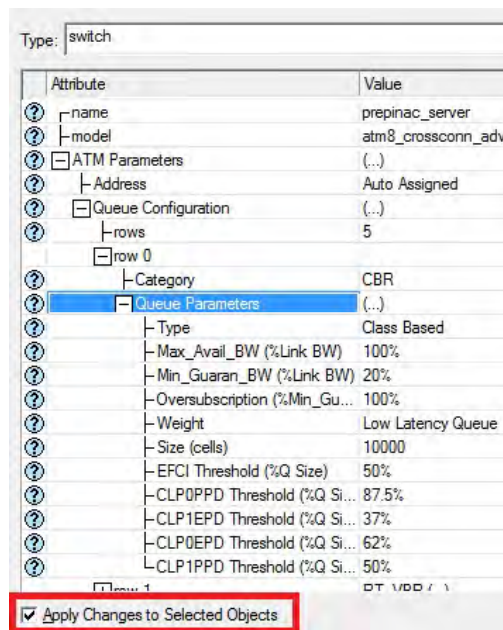
- **client\_FTP:**

<sup>28</sup> Pro hlasové aplikace by správně měl být nastaven adaptační protokol AAL1, ale ten u verze IT Guru není podporován. Proto volíme AAL2.

- *Application: Supported Profiles* --> „FTP\_prof“
- *Application:Destination Preferences* --> „FTP Server“/„server\_FTP“
- *ATM Application Parameters* --> „ABR only“
- *ATM Parameters/Queue Configuration* --> „ABR Only (Per VC Queue)“
- **client\_EMAIL:**
  - *Application: Supported Profiles* --> „EMAIL\_prof“
  - *Application:Destination Preferences* --> „EMAIL Server“/„server\_EMAIL“
  - *ATM Application Parameters* --> „ABR only“
  - *ATM Parameters/Queue Configuration* --> „ABR Only (Per VC Queue)“
- **client\_voice\_1:**
  - *Application: Supported Profiles* --> „VOICE\_prof“
  - *Application: Supported Services* --> „VOICE\_app“
  - *Application: Destination Preferences* --> „Voice Destination“/„client\_voice\_2“
  - *ATM Application Parameters* --> „CBR only“
  - *ATM Parameters/Queue Configuration* --> „CBR Only“
  - *Application: Transport Protocol/Voice Transport* --> „AAL2“
- **client\_voice\_2:**
  - *Application: Supported Profiles* --> „VOICE\_prof“,
  - *Application: Supported Services* --> „VOICE\_app“,
  - *Application: Destination Preferences* --> „Voice Destination“/„client\_voice\_1“
  - *ATM Application Parameters* --> „CBR only“
  - *ATM Parameters/Queue Configuration* --> „CBR Only“
  - *Application: Transport Protocol/Voice Transport* --> „AAL2“
- **server\_FTP:**
  - *Application: Supported Services* --> „FTP\_app“
  - *ATM Application Parameters* --> „ABR only“

- *ATM Parameters/Queue Configuration --> „ABR Only (Per VC Queue)“*
- **server\_EMAIL:**
  - *Application: Supported Services --> „EMAIL\_app“*
  - *ATM Application Parameters --> „ABR only“*
  - *ATM Parameters/Queue Configuration --> „ABR Only (Per VC Queue)“*

20. Na obou přepínačích bude shodné nastavení. Označte tedy oba přepínače a vstupte do nastavení jednoho z nich. U třídy služeb CBR nastavte položku *Max\_Avail\_BW (%Link BW)* na hodnotu 100 % a položku *Min\_Guaran\_BW (%Link BW)* na hodnotu 20 %. (Obr. 10.12). Tím docílíme toho, že datový provoz využívající třídu služeb CBR bude mít garantováno minimálně 20 % kapacitu spoje a bude moci obsadit až 100 % kapacity. Před potvrzením je nutné ještě zaškrtnout červeně označené pole *Apply Changes to Selected Objects*, aby se nastavení projevilo na obou prvcích.




Obr. 10.12: Nastavení třídy služeb CBR na přepínačích.

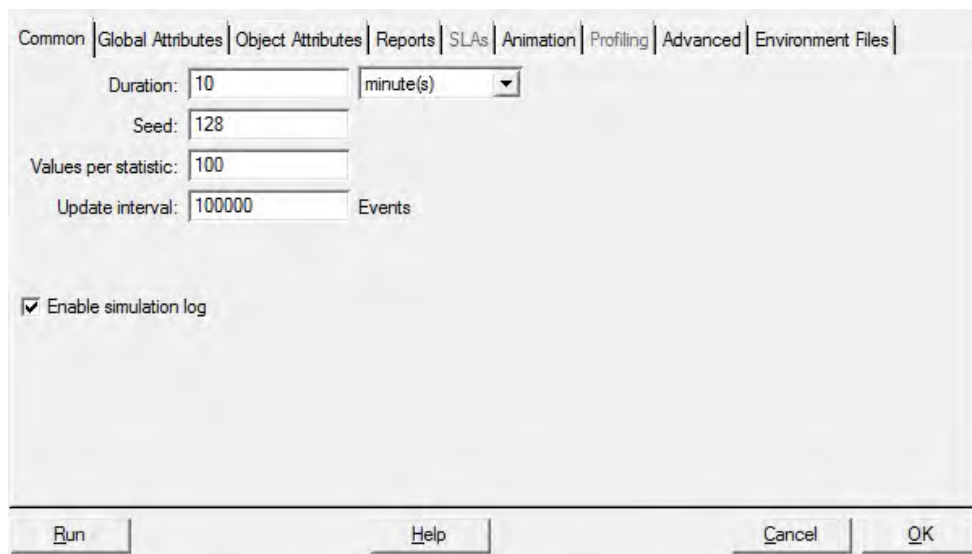
21. Po nakonfigurování základní topologie a jednotlivých komponent přistupte k vybrání statistik, které budete sledovat. Statistiku vyberete kliknutím pravého

tlačítka myši na plochu a z nabídky vyberete *Choose Individual Statistics*. Většinu statistik budete nastavovat globálně pro celou síť. Statistiky, u nichž je v závorce uvedeno upřesnění konkrétního prvku, nastavíte obdobným způsobem, ovšem pro vybrání statistiky pouze na požadovaném prvku, kliknete pravým tlačítkem myši na daný prvek a opět vyberete možnost *Choose Individual Statistics*.

Z nabízených statistik vyberte následující:

- a) Global Statistics: ATM/Cell Delay (sec)
  - ATM/Cell Delay Variation
  - Email/Download Response Time (sec)
  - FTP/ Download Response Time (sec)
  - Voice/Packet Delay Variation
  - Voice/Packet End-to-End Delay (sec)
- b) Node Statistics: Server Ftp/ Traffic Sent (bytes/sec)
  - Server Ftp/ Traffic Received (bytes/sec)
  - Client Email/ Download Response Time (sec)
  - Client Email/ Traffic Received (bytes/sec)
  - Client Email/ Traffic Sent (bytes/sec)
  - Client Ftp/ Download Response Time (sec)
  - Client Ftp/ Traffic Received (bytes/sec)
  - Client Ftp/ Traffic Sent (bytes/sec)
  - Voice Application/ Packet End-to-End Delay (sec)
  - Voice Application/ Traffic Received (bytes/sec)
  - Voice Application/ Traffic Sent (bytes/sec)
- c) Link Statistics: point-to-point/utilization <-- (spoj mezi přepínači)
  - point-to-point/utilization --> (spoj mezi přepínači)

22. Po vybrání sledovaných statistik můžete přistoupit k vlastní simulaci. Stisknutím ikony  (Run) se dostanete do konfiguračního okna simulace, kde nastavte čas simulace na 10 minut, počet hodnot na statistiku 100 a obnovovací interval na 100000 hodnot. (Obr. 10.13) Po nastavení požadovaných parametrů stiskněte tlačítko **Run** pro zahájení simulace.



Obr. 10.13: Nastavení parametrů simulace.

23. Pro zobrazení výsledků klikněte pravým tlačítkem myši na plochu a z nabídky vyberte *View Results*. Po vybrání statistik:

*Global Statistics/Email/Download Response Time (sec),*

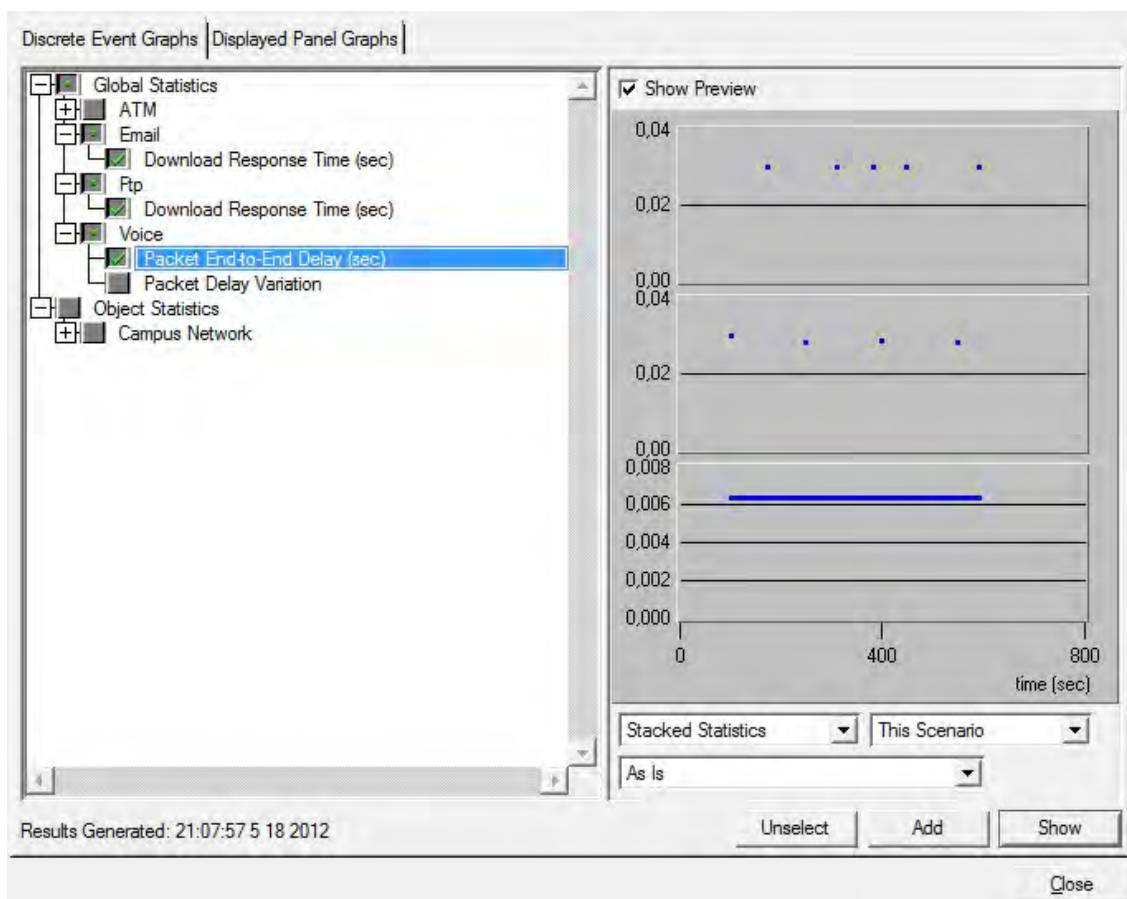
*Global Statistics/FTP/Download Response Time (sec),*

*Global Statistics/Voice/Packet End-to-End Delay (sec),*

byste měli vidět shodné grafy jako na obrázku 10.14.<sup>29</sup>

---

<sup>29</sup> Graf lze zobrazit po zmáčknutí tlačítka **Show** a v grafu pomocí kurzoru myši vybrat požadovanou oblast pro přiblížení. Pro navrácení zobrazení celého grafu můžete využít pravé tlačítko myši a vybrat „Full Horizontal Scale“ a „Full Vertical Scale“.



Obr. 10.14: Ukázka okna se statistikami pro úvodní scénář.

24. Po úspěšném zobrazení grafu a ověření správnosti nakonfigurování jednotlivých prvků rozšířte projekt o další scénář. K vytvoření nového scénáře využijte možnost duplikování současného scénáře. Toho docílíte vybráním z menu *Scenarios/Duplicate Scenario* a zadáním jména nového scénáře. Nový scénář pojmenujte „ATM\_CBR\_UBR\_0“.<sup>30</sup> Jak z názvu scénáře vyplývá, pro hlasovou aplikaci bude stále využívána třída CBR. Naopak pro datové aplikace FTP a Email bude využita třída UBR.
25. Na klientech a serverech s podporou datových aplikací tedy musíte změnit třídu služeb z ABR na CBR. Ke změně parametrů využívejte opět hromadného nastavení parametrů pomocí výběru prvků se stejnými změnami (Ctrl + kliknutí levého tlačítka myši) a zaškrtnutí políčka *Apply Changes to Selected Objects* před potvrzením nastavení. Označte si tedy všechny 4 prvky, na kterých je nastavena

<sup>30</sup> Pro změnu scénáře lze využít položky menu *Scenarios/Switch To Scenario...*

podpora aplikace FTP nebo Email (2x klient a 2x server) a vstupte do konfigurace jednoho z nich. Změňte položku *ATM Application Parametrs* na hodnotu „*UBR only*“ a *ATM Parametrs/Queue Configuration* na „*UBR*“. (Obr. 10.15) Zatrhněte políčko *Apply Changes to Selected Objects* a nastavení potvrďte.

Attribute	Value
? -name	client_FTP
? -model	atm_uni_client_adv
? + ATM Application Parameters	UBR Only
? - ATM Parameters	(...)
? - Address	Auto Assigned
? + Queue Configuration	UBR
? + Per-Port Configuration	(...)

Obr. 10.15: Nastavení třídy služeb UBR.

26. Nově vytvořený scénář „ATM\_CBR\_UBR\_0“ opět duplikujte výběrem položky *Scenarios/Duplicate Scenario* a zadáním jména nového scénáře. Nový scénář pojmenujte „ATM\_UBR\_all\_0“. Pro veškerý provoz v síti tedy bude využívána třída služeb UBR. Stačí tedy v nově vytvořeném scénáři zajistit podporu UBR třídy služeb u hlasové aplikace, viz další krok. U ostatních aplikací je již UBR nastaveno z minulého scénáře.
27. Budete nastavovat oba klienty s podporou *voice* aplikace (client\_voice\_1 a client\_voice\_2). Označte si oba klienty a vstupte do nastavení jednoho z nich. Změňte položku *ATM Application Parametrs* na hodnotu „*UBR only*“ a *ATM Parametrs/Queue Configuration* na „*UBR*“. (Obr. 10.15) U položky *Application:Transport Protocol/Voice Transport* vyberte protokol „*AAL5*“. Zatrhněte políčko *Apply Changes to Selected Objects* a nastavení potvrďte.
28. Po nakonfigurování dalších scénářů je nutné znovu simulovat chování sítě. K tomu nyní nevyužívejte tlačítko Run jako v předchozím případě, ale vyberte z nabídky *Scenarios/Manage Scenarios...* a u položek *Results* vyberte pro nově vytvořené scénáře <collect> respektive <recollect>, jak znázorňuje Obr. 10.16. Délku simulace ponechte 10 minut a potvrďte volbu tlačítkem **OK**.

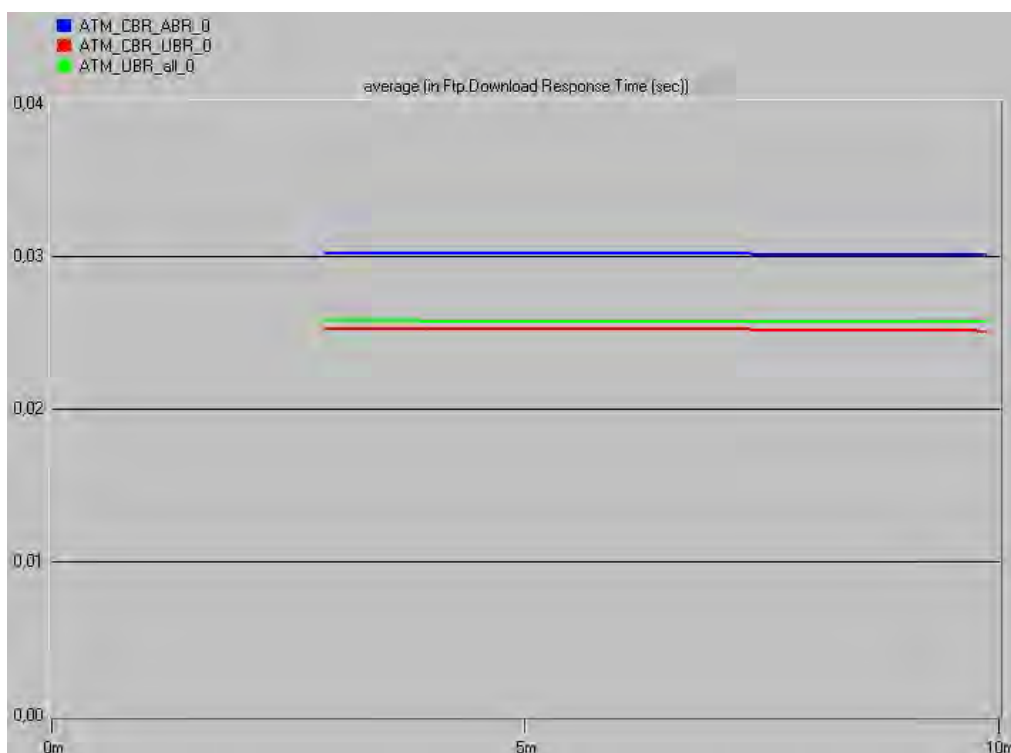


Project Name:

#	Scenario Name	Saved	Results	Sim Duration	Time Units
1	ATM_CBR_ABR_0	saved	out of date	10	minute(s)
2	ATM_CBR_UBR_0	saved	<recollect>	10	minute(s)
3	ATM_UBR_all_0	saved	<recollect>	10	minute(s)

Obr. 10.16: Nastavení parametrů simulace.

29. Pro kontrolu správného nastavení nově vytvořených scénářů si zobrazte výsledky simulace kliknutím pravého tlačítka myši na plochu a vybráním „View Results“. Pro zobrazení více položek do jednoho grafu vyberte „Overlaid Statistics“. Pro zobrazení všech scénářů vyberte hodnotu „All Scenarios“. U některých druhů statistik je vhodné zvolit průměrování hodnot „average“. Po vybrání statistiky *Global Statistik/FTP/Download Response Time (sec)* byste měli vidět statistiku shodnou s obrázkem 10.17.



Obr. 10.17: Ukázka statistiky *Download Response Time (sec)* pro FTP aplikaci.



### 10.1.2 Doplnující otázky a úkoly<sup>31</sup>

- 1) Prohlédněte si jednotlivé nakonfigurované statistiky a porovnejte chování sítě pro jednotlivé třídy služeb. Zaměřte se zejména na statistiku *Global Statistic/Voice/Packet End-to-End Delay (sec)*.
- 2) Známým postupem duplikujte scénáře „ATM\_CBR\_UBR\_0“ a „ATM\_UBR\_all\_0“<sup>32</sup> a na spoji mezi přepínači nastavte provoz na pozadí 70 % od času 150 s. Nové scénáře pojmenujte shodně s původními, pouze místo 0 na konci názvu zadáte 70. (Pro scénář „ATM\_CBR\_UBR\_0“ tedy nový název bude „ATM\_CBR\_UBR\_70“) Provoz na pozadí nastavíte v nastavení atributů spoje. (*Edit Attributes*). (Obr. 10.18) Po simulování nově vytvořených scénářů si zobrazte výsledky simulace a diskutujte vliv zatížení sítě na chování sítě.<sup>33</sup>

Attribute	Value
name	prepinac_client <-> prepinac_server
model	ATM_adv
port a	prepinac_client.ATM (P3)
port b	prepinac_server.ATM (P0)
ATM Link Failure Report Export	Do Not Export
ATM Trunk Report Export	Do Not Export
Aggregation Token	0
Background Utilization	(...)
rows	1
row 0	
time (sec)	150
background utilization (%)	70
direction	A <-> B
Fiber Segments	None
Propagation Speed	Speed of Light
data rate	DS1

Obr. 10.18: Nastavení provozu na pozadí na spoji mezi přepínači.

- 3) Duplikujte dva nově vytvořené scénáře v předchozím úkolu (adekvátně pojmenujte) a nastavte u nich vytížení spoje na 90 %<sup>34</sup> opět v čase 150 s.

<sup>31</sup> Odpovědi na otázky si poznamenejte a na konci cvičení je přednesete vyučujícímu.

<sup>32</sup> Se scénářem „ATM\_CBR\_ABR\_0“ již nebudete dále pracovat z důvodu minimálních rozdílů ve statistikách se scénářem „ATM\_CBR\_UBR\_0“. Při simulaci nových scénářů proto můžete zvolit možnost <discard> místo <collect> u položky *results* v okně *Manage Scenarios*.

<sup>33</sup> Pro zobrazení statistik pouze pro některé scénáře je vhodné využít možnost *Selected Scenarios* v nastavení pod grafem.

<sup>34</sup> Reálná síť se považuje za vytíženou při zatížení přibližně 70 %. Nastavená hodnota 90 % je zvolena pro názornou ukázkou chování sítě při extrémním zatížení.

Opět si zobrazte výsledky simulace a diskutujte vliv takto extrémního zatížení sítě.

- 4) Scénáře s provozem na pozadí 70 % opět duplikujte a nastavíte u nich zvýšenou zátěž pro datové aplikace.<sup>35</sup> Pro nové scénáře zvolte jméno např. „ATM\_CBR\_UBR\_70\_high\_load“ a „ATM\_UBR\_all\_70\_high\_load“. Pro nastavení zvýšené zátěže vstoupíte do nastavení prvku „app\_config“ a u FTP a EMAIL aplikace zvolíte možnost „High Load“, viz Obr. 10.19. U tohoto úkolu se zaměřte zejména na zpoždění a kolísání zpoždění pro hlasovou aplikaci.

Attribute	Value
[-] Application Definitions	(...)
[-] rows	3
[-] row 0	
[-] Name	FTP_app
[-] Description	(...)
[-] Custom	Off
[-] Database	Off
[-] Email	Off
[-] Ftp	High Load
[-] Http	Off
[-] Print	Off
[-] Remote Login	Off
[-] Video Conferencing	Off
[-] Voice	Off
[-] row 1	
[-] Name	EMAIL_app
[-] Description	(...)
[-] Custom	Off
[-] Database	Off
[-] Email	High Load
[-] Ftp	Off

Obr. 10.19: Nastavení zvýšené zátěže pro aplikace FTP a EMAIL.

## 10.2 Úkol 2 – Frame Relay

Druhá část této úlohy je zaměřena na technologii Frame Relay. Topologie úlohy zůstane podobná, pouze s ohledem na danou technologii do sítě budou vloženy 2 směrovače, mezi kterými budou vytvořeny trvalé virtuální okruhy (PVC) pro jednotlivé

<sup>35</sup> Nastavení provozu na pozadí v prostředí IT Guru v podstatě znamená pouze snížení propustnosti linky např. o 70 %, což samozřejmě není zcela reálné chování zatížení linky. Tato možnost byla zvolena s ohledem na rozsah úlohy tak, aby se nemusel zdlouhavě přidávat další síťový provoz, proto v posledním doplňujícím úkolu nastavujete zvýšený provoz pro datové aplikace.

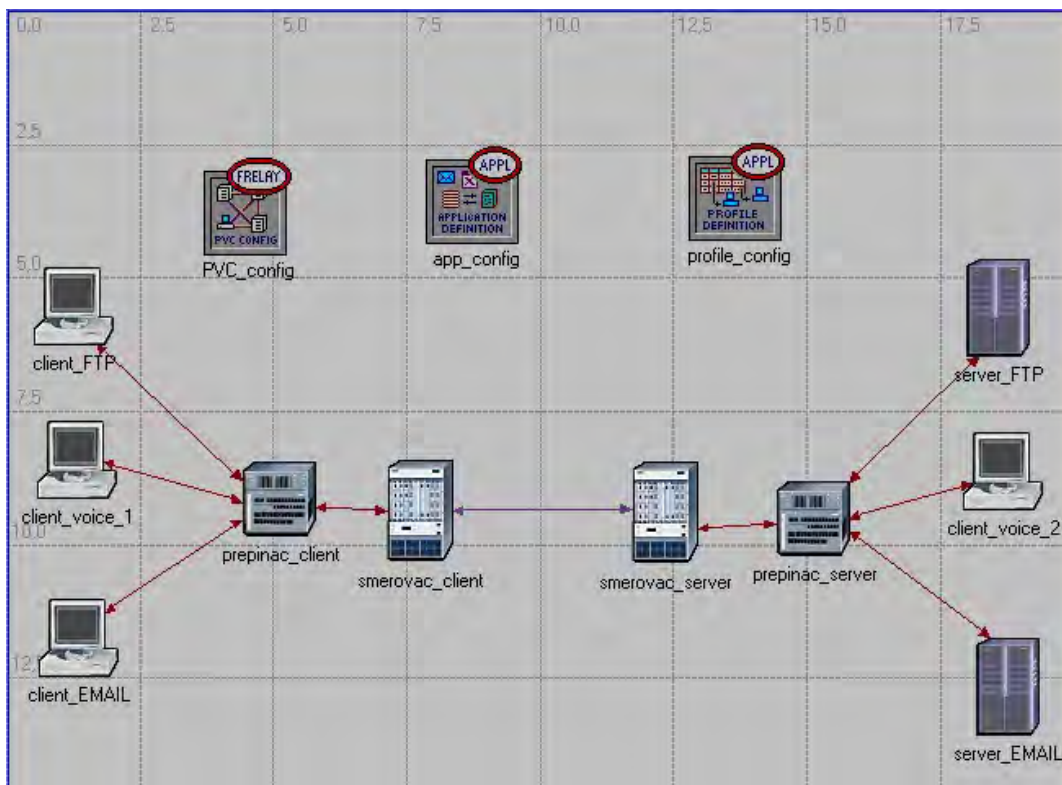
aplikace s odlišným typem provozu ToS (*Type of Services*). V nových scénářích využijete aplikace a profily pro aplikace vytvořené v předchozí části úlohy.

### 10.2.1 Postup

1. Scénář „ATM\_CBR\_UBR\_0“ duplikujte výběrem položky z menu programu *Scenarios/Duplicate Scenario* a zadáním jména nového scénáře. Nový scénář pojmenujte „FR\_data\_best\_effort\_0“.<sup>36</sup>
2. V nově vytvořeném scénáři smažte všechny prvky kromě „app\_config“ a „profile\_config“. Nastavené aplikace využijete i v této části úlohy.
3. Vložte na plochu postupně tyto komponenty z okna *Object Palette*:
  - I. 4x ethernet\_wkstn
  - II. 2x ethernet\_server
  - III. 2x přepínač ethernet16\_switch
  - IV. 2x směrovač fr4\_ethernet2\_gtwy
  - V. 1x FR PVC Config
4. Směrovače propojte technologií „FR\_T1“ a zbylé prvky v síti propojte technologií „100BaseT“, viz Obr. 10.20. Jednotlivé prvky podle obrázku **pojmenujte** a **nastavte adresy pro servery a klienty** opět shodné s názvy prvků (totožné s první částí úlohy).

---

<sup>36</sup> Význam jednotlivých položek v názvu je podobný jako u první části úlohy. Část „FR“ značí, že je nakonfigurován protokol Frame Relay, druhá část „data\_best\_effort“ označuje použité ToS u datových aplikací FTP a EMAIL a „0“ opět znamená, že není nastaven žádný provoz na pozadí.



Obr. 10.20: Základní topologie pro Frame Relay.

5. Po vytvoření základní topologie opět musíte zajistit podporu vytvořených aplikací a profilů na jednotlivých prvcích. Postup i nastavení bude shodné jako v první části úlohy, proto bude uveden pouze stručný přehled nastavení pro jednotlivé prvky.

- **client\_FTP:**
  - *Application: Supported Profiles* --> „FTP\_prof“
  - *Application: Destination Preferences* --> „FTP Server“/„server\_FTP“
- **client\_EMAIL:**
  - *Application: Supported Profiles* --> „EMAIL\_prof“
  - *Application: Destination Preferences* --> „EMAIL Server“/„server\_EMAIL“
- **client\_voice\_1:**
  - *Application: Supported Profiles* --> „VOICE\_prof“,
  - *Application: Supported Services* --> „VOICE\_app“,
  - *Application: Destination Preferences* --> „Voice Destination“/„client\_voice\_2“
- **client\_voice\_2:**

- *Application: Supported Profiles* --> „VOICE\_prof“,
- *Application: Supported Services* --> „VOICE\_app“,
- *Application: Destination Preferences* --> „Voice Destination“/  
„client\_voice\_1“

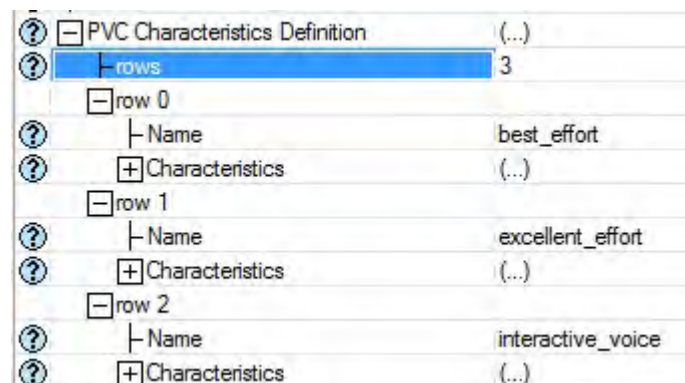
- **server\_FTP:**

- *Application: Supported Services* --> „FTP\_app“

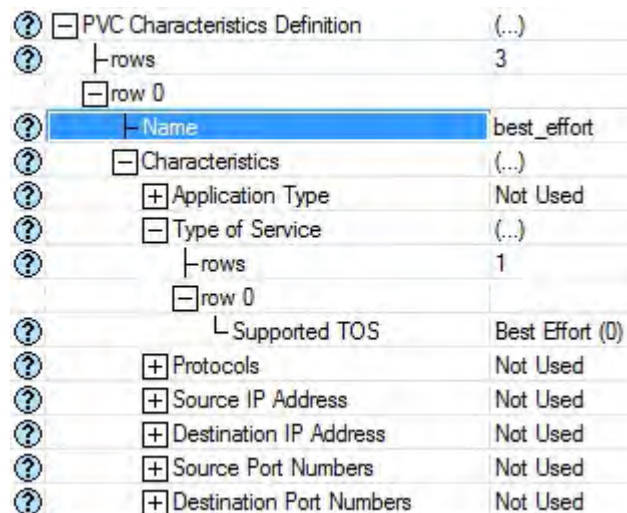
- **server\_EMAIL:**

- *Application: Supported Services* --> „EMAIL\_app“

6. Pro Frame Relay spojení je nutné vytvořit virtuální okruh, který budete nastavovat mezi dvěma směrovači. Nejprve nastavíte prvek „PVC\_config“, v kterém definujete parametry jednotlivých virtuálních spojů. Vstupte proto do nastavení parametrů daného prvku a definujte 3 nové PVC spoje. Pojmenujte je „excellent\_effort“, „best\_effort“ a „interactive\_voice“ (Obr. 10.21). U jednotlivých spojů nastavte u položky „*Type of Service*“, třídu podle názvu daného spoje. Nastavení pro „best\_effort“ můžete zkontrolovat s obrázkem 10.22.

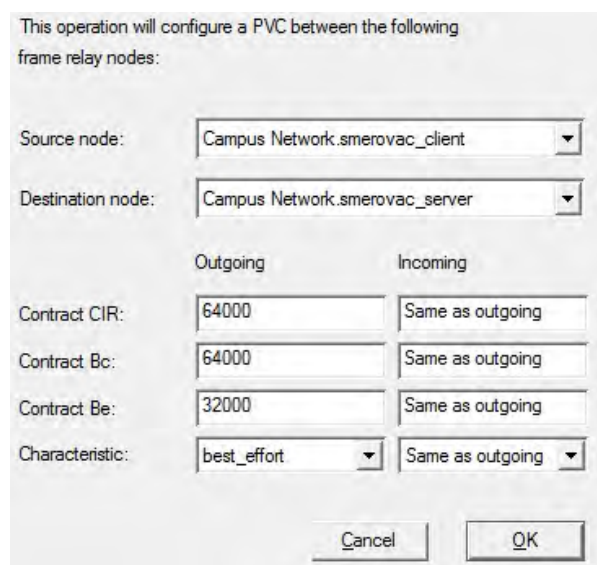


Obr. 10.21: Nastavení názvů PVC spojů.



Obr. 10.22: Určení typu provozu *Best Effort (0)*.

- Nyní využijete nastavené parametry spojů k vytvoření vlastních spojů mezi směrovači. Označte si oba směrovače a z menu programu vyberte možnost *Protocols/Frame Relay/Configure a PVC between Selected Nodes...* V nově otevřeném okně zadáte parametry spoje podle obrázku 10.23.



Obr. 10.23: Nastavení PVC pro best\_effort.

- Spoje vytvoříte i pro zbylé dva předkonfigurované spoje „excellent\_effort“ (Obr. 10.24) a „interactive\_voice“ (Obr. 10.25).

This operation will configure a PVC between the following frame relay nodes:

Source node: Campus Network.smerovac\_client

Destination node: Campus Network.smerovac\_server

	Outgoing	Incoming
Contract CIR:	64000	Same as outgoing
Contract Bc:	64000	Same as outgoing
Contract Be:	32000	Same as outgoing
Characteristic:	excellent_effort	Same as outgoing

Cancel OK

Obr. 10.24:Nastavení PVC pro excellent\_effort.

This operation will configure a PVC between the following frame relay nodes:

Source node: Campus Network.smerovac\_client

Destination node: Campus Network.smerovac\_server

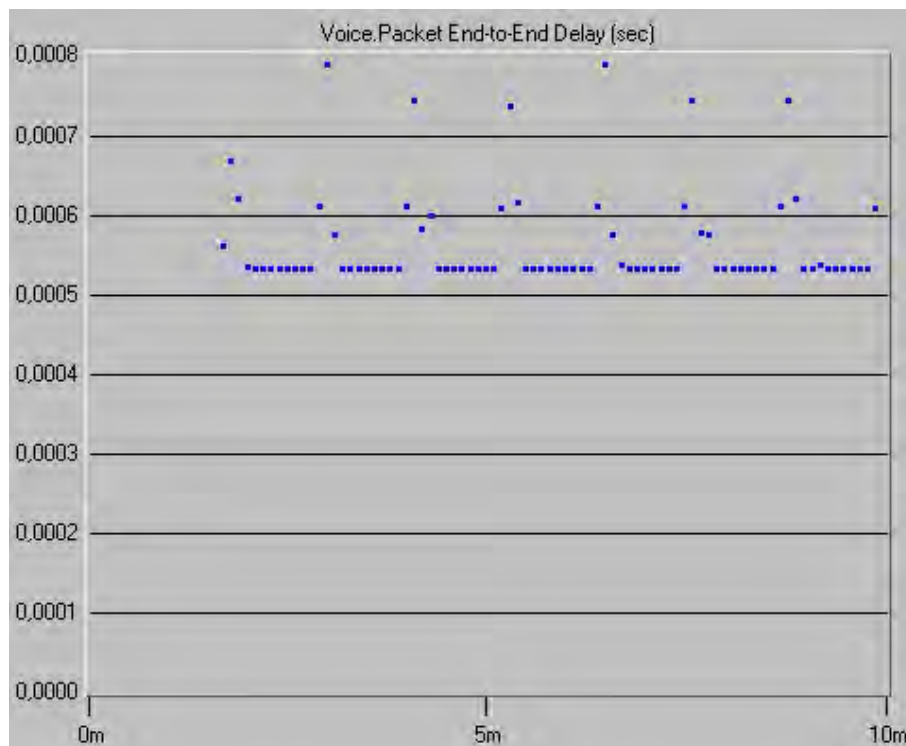
	Outgoing	Incoming
Contract CIR:	256000	Same as outgoing
Contract Bc:	256000	Same as outgoing
Contract Be:	1288000	Same as outgoing
Characteristic:	interactive_voice	Same as outgoing

Cancel OK

Obr. 10.25: Nastavení PVC pro interactive\_voice.

9. Po vybrání nastavení nového scénáře musíte znovu simulovat chování sítě. K tomu využijte nabídku menu *Scenarios/Manage Scenarios...* a u položky *Results* vyberte *<collect>* respektive *<recollect>* pouze pro nově konfigurovaný scénář.
10. K ověření správnosti nakonfigurování tohoto úkolu využijte statistiku *Global Statistics/Voice/Packet End-to-End Delay (sec)* a porovnejte ji s obrázkem 10.26. Výsledky simulace zobrazíte kliknutím pravého tlačítka myši na plochu a výběrem možnosti *View Results*.





Obr. 10.26: Zpoždění pro hlasovou aplikaci v s/min.

11. Scénář „FR\_data\_best\_effort\_0“ duplikujte a nový scénář nazvěte „FR\_all\_best\_effort\_0“. U tohoto nového scénáře pro hlasovou aplikaci nastavíte položku ToS na *Best Effort*. Vstupte proto do nastavení prvku „app\_config“ a pro aplikaci „VOICE\_app“ u položky *Application Definitions/Description/Voice* nastavte položku *Type of Service* na hodnotu „*Best Effort (0)*“, viz Obr. 10.27.

Attribute	Value
Silence Length (seconds)	default
Talk Spurt Length (seconds)	default
Symbolic Destination Name	Voice Destination
Encoder Scheme	G.711
Voice Frames per Packet	1
Type of Service	Best Effort (0)
RSVP Parameters	None

Obr. 10.27: Nastavení třídy *Best Effort* pro hlasovou aplikaci.



### 10.2.2 Doplnující otázky a úkoly

- 1) Zobrazte si statistiku *Global Statistics/Voice/Packet End-to-End Delay (sec)* pro scénář „FR\_data\_best\_effort\_0“ a porovnejte hodnoty se scénářem „ATM\_CBR\_UBR\_0“.
- 2) Statistiku *Global Statistics/Voice/Packet End-to-End Delay (sec)* si zobrazte i pro oba vytvořené scénáře Frame Relay „FR\_data\_best\_effort\_0“ a „FR\_all\_best\_effort\_0“.<sup>37</sup> Diskutujte průběh statistiky.
- 3) Kolik a jaké třídy služeb podporují technologie ATM a Frame Relay? Třídy stačí vyjmenovat.

---

<sup>37</sup> Pro diskuzi k tomuto doplňujícímu úkolu je vhodné se podívat i na statistiku odeslaných/přijatých dat na jednotlivých klientech s podporou hlasové aplikace.

# ZÁVĚR

Cílem diplomové práce bylo vypracovat návrh laboratorních úloh zabývajících se základními síťovými technologiemi a protokoly v prostředí OPNET. K návrhu laboratorních úloh byla vybrána verze programu OPNET IT Guru Academic Edition 9.1.A, která studentům poskytuje výhodu v podobě bezplatného využívání, na úkor omezené funkčnosti programu oproti jeho plně placené verzi. Při vytváření laboratorních úloh na tuto skutečnost musel být brán zřetel, což v určitých případech bylo limitující, ale celkově tato verze pro základní síťové technologie dostačovala. Úvodní část projektu je věnována seznámení se s vývojovým prostředím OPNET a síťovými technologiemi a protokoly použitými při návrhu laboratorních úloh pro předmět Komunikační technologie.

Navržené laboratorní úlohy byly sestaveny tak, aby studentům druhého ročníku bakalářského studia poskytly vhodnou pomůcku pro pochopení dané problematiky a pomohly pochopit rozdíly mezi jednotlivými protokoly a technologiemi. V práci byly navrženy 4 laboratorní úlohy. Ke každé úloze byl vytvořen podrobný návod pro studenty k sestavení programu. Návod k laboratorním úlohám jsou členěny do logických částí (úkolů) a ke každé části je v návodu uvedeno několik doplňujících otázek a úkolů. Návod jsou koncipovány tak, aby studentům co nejdetailněji ukázaly postup pro vytvoření požadovaných simulací, studenti se však při vypracování doplňujících otázek a úkolů musejí nad danou problematikou zamyslet, aby to vedlo k pochopení dané problematiky. Odpovědi na doplňující otázky a úkoly by studenti měli na konci cvičení prezentovat cvičícímu.

Součástí diplomové práce jsou i vzorová řešení navržených úloh. Vzorová řešení laboratorních úloh jsou umístěny do příloh diplomové práce a zdrojové kódy k vytvořeným programům jsou uloženy na přiloženém CD.

# LITERATURA

- [1] FOROUZAN, B. A. TCP/IP Protocol Suite, McGraw-Hill Higher Education, Boston, 4. vydání, 2010. 979 s.
- [2] HEDRICK, C. Routing Information Protocol, RFC 1058. Rutgers University, Červen 1988. 26s. [cit. 2012-02-02]. Dostupné z URL: <<http://www.faqs.org/rfcs/rfc1058.html>>.
- [3] JEŘÁBEK, J. Pokročilé komunikační techniky, Skriptum FEKT VUT v Brně, 2011. 248 s.
- [4] KOLÁŘ, Josef. Teoretická informatika. 2. vyd. Česká informatická společnost, Praha, 2004. 205 s, ISBN 80-900853-8-5.
- [5] MALKIN, G. RIP Version 2, RFC 2453. Bay Networks, Listopad 1998. 29 s. [cit. 2012-05-02]. Dostupné z URL: < <http://www.faqs.org/rfcs/rfc2453.html> >.
- [6] MALKIN, G. RIPng for IPv6, RFC 2080. Ipsilon Networks, Leden 1997. 19 s. [cit. 2012-04-17]. Dostupné z URL: < [http:// http://www.faqs.org/rfcs/rfc2080.html](http://http://www.faqs.org/rfcs/rfc2080.html)>.
- [7] MOY, J. OSPF Version 2, RFC 1247. Proteon, Inc. Červenec 1991. 134 s. [cit. 2012-03-17]. Dostupné z URL: < <http://www.faqs.org/rfcs/rfc1247.html> >.
- [8] MOY, J. OSPF Version 2, RFC 2328. Ascend Communications, Inc. Duben 1998. 155 s. [cit. 2012-04-06]. Dostupné z URL: < <http://www.faqs.org/rfcs/rfc2328.html> >.
- [9] NOVOTNÝ, V. Architektura sítí, Skriptum FEKT VUT v Brně, 2002. 136 s.
- [10] OPNET Technologies, OPNET IT Guru Documentation Academic Edition 9.1.A PL1, 2010.
- [11] OPNET Technologies, OPNET Modeler Product Documentation Release 16.0, 2010.
- [12] PETERKA, Jiří. Počítačová encyklopedie: ATM - Asynchronous Transfer Mode. *CHIPweek* [online]. 15.9.1998, 38/98 [cit. 2012-04-17]. Dostupné z URL: <http://www.earchiv.cz/a98/a838k180.php3>
- [13] POSTEL, J. User Datagram Protocol, RFC 768, Information Sciences Institute, 29.8.1980. 3 s. [cit. 2012-05-18]. Dostupné z URL: < <http://www.faqs.org/rfcs/rfc768.html>>.
- [14] PUŽMANOVÁ, Rita. Ethernet s kapacitou 40 a 100 Gbit/s. *Elektrotechnický magazín* [online]. 2010, 9/2010, [cit. 2011-12-15]. Dostupný z URL: <[http://www.cesnet.cz/sdruzeni/napsali-o-nas/2010/09/201009\\_ETM.html](http://www.cesnet.cz/sdruzeni/napsali-o-nas/2010/09/201009_ETM.html)>.

- [15] RFC 793. Transmission Control Protocol. University of Southern California : Information Sciences Institute, Září 1981. 85 s. [cit. 2012-05-03]. Dostupné z URL: <<http://www.faqs.org/rfcs/rfc793.html>>.
- [16] Slaviček, K. ATM. Zpravodaj ÚVT MU. ISSN 1212-0901, 1996, roč. VI, č. 4, s. 14-17. [cit. 2012-03-10]. Dostupné z URL: <<http://www.ics.muni.cz/bulletin/articles/68.html>>.

# SEZNAM POUŽITÝCH ZKRATEK

AAL – ATM Adaptation Layer

ABR – Area Border Router

ABR – Available Bit Rate

AFI – Address Family Identifier

ATM – Asynchronous Transfer Mode

BDR – Backup Designated Router

B-ISDN – Broadband Integrated Services Digital Network

CBR – Constant Bit Rate

CCK – Complementary Code Keying

CSMA/CA – Carrier Sense Multiple Access with Collision Avoidance

CSMA/CD – Carrier Sense Multiple Access with Collision Detection

DCE – Data Circuit-terminating Equipment

DLCI – Data-link Connection Identifier

DNS – Domain Name Server

DR – Designated Router

DSSS – Direct Sequence Spread Spectrum

DTE – Data Terminal Equipment

EGP – Exteriér Gateway Routing Protocol

FCS – Frame Check Sequence

Gbit/s – přenosová rychlost v giga bitech za sekundu

IEEE – Institute of Electrical and Electronic Engineers

IGP – Interior Gateway Routing Protocol

IP – Internet Protocol

ISM – Industrial, Scientific and Medical

ISN – Initial Sequence Number

LAN – Local Area Network

Mbit/s – přenosová rychlost v mega bitech za sekundu

MIMO – Multiple Input and Multiple Output

OFDM – Orthogonal Frequency Division Multiplexing

OSPF – Open Shortest Path First

PVC – Permanent Virtual Circuit

RIP – Routing Information Protocol

SVC – Switched Virtual Circuit

TCP – Transmission Control Protocol

UBR – Unspecified Bit Rate

UDP – User Datagram Protocol

VBR – Variable Bit Rate

VCI – Virtual Channel Identifier

VoIP – Voice Over Internet Protocol

VPI – Virtual Path Identifier

WAN – Wide Area Network

Wi-Fi – Wireless Fidelity

WLAN – Wireless Local Area Network

# SEZNAM PŘÍLOH

- A – Vzorové řešení laboratorní úlohy Srovnání protokolů TCP a UDP.
- B – Vzorové řešení laboratorní úlohy Srovnání WLAN s Ethernetem.
- C – Vzorové řešení laboratorní úlohy Směrovací protokoly.
- D – Vzorové řešení laboratorní úlohy Technologie ATM a Frame Relay.
- E – Obsah přiloženého CD.

# A ŘEŠENÍ PRO SROVNÁNÍ PROTOKOLŮ TCP A UDP

Tato laboratorní úloha je zaměřena na porovnání dvou základních protokolů transportní vrstvy. Protokol TCP je označován jako protokol pro spolehlivý (potvrzovaný) přenos dat. Na druhé straně protokol UDP je jednoduchý protokol používaný u jednoduchých aplikací typu dotaz-odpověď nebo u aplikací, které nejsou kritické na ztrátu paketů během přenosu.

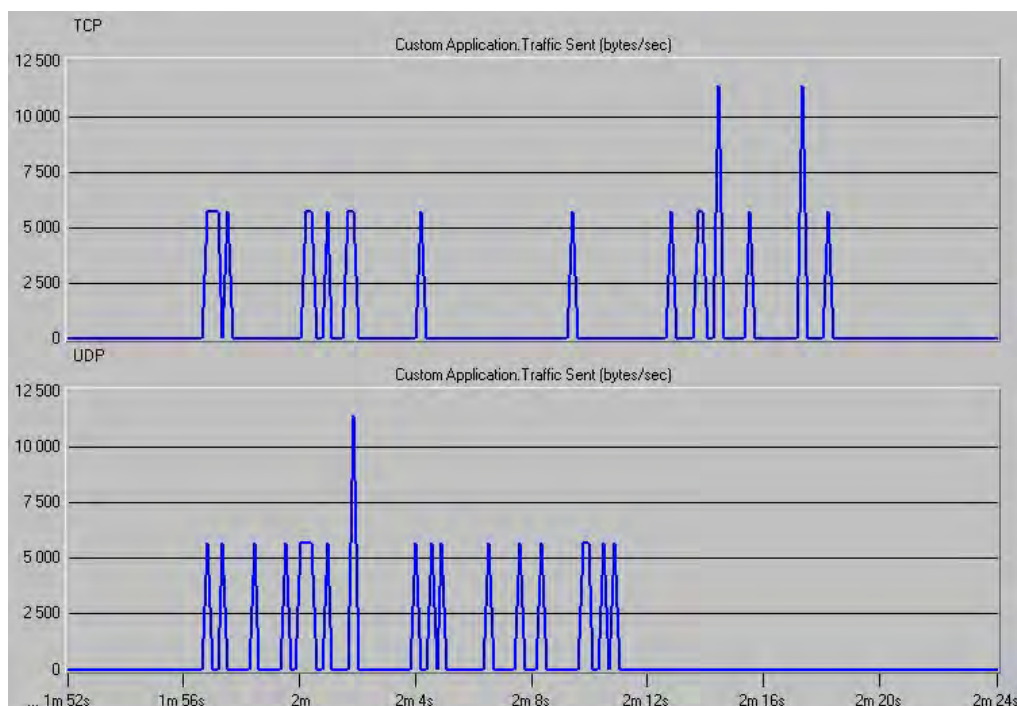
## A.1 Úkol 1

V prvním části úlohy byla vytvořena základní topologie s nastavením jednotlivých komponent. Pro vytvoření síťového provozu byla použita komponenta *Task*, pomocí které je možné si nadefinovat vlastní síťový provoz, což bylo vhodné, jelikož oba transportní protokoly jsou vhodné a využívány odlišnými aplikacemi. Byly vytvořeny dva scénáře, v každém byl použit jiný transportní protokol.

Doplňující otázky a úkoly:

- 1) Tento doplňující úkol je zaměřen na seznámení s výsledky simulace.
- 2) Na obrázku A.1 je možné vidět statistiku, z které je patrné, že pro scénář, v němž je použit transportní protokol TCP, potřebuje k přenosu shodného objemu dat delší dobu, což je zapříčiněno vlastnostmi protokolu TCP jako je navazování a potvrzování spojení.





Obr. A.1: Statistika pro celková odeslaná data vlastní aplikací.

- 3) Fakt, že v IP statistikách jednotlivých klientů je možné pozorovat provoz pro oba transportní protokoly je dán posloupností zapouzdřování dat podle TCP/IP modelu. Protokol IP je protokol síťové vrstvy, a tudíž je pod transportními protokoly.
- 4) UDP protokol je protokol, který je označován jako nespolehlivý a nespojovaný a využívají jej zejména aplikace pro hlasové služby, online hry, ale například i směrovací protokol RIP, čehož je možné si všimnout i ve výsledcích simulace při inicializaci spojení. (Po přednastaveném čase je protokol RIP vypnut, aby neovlivňoval výsledky simulace)  
 Protokol TCP je naopak používán všude tam, kde potřebujeme spolehlivou, potvrzovanou službu. Aplikace, které jako transportní protokol využívají právě TCP, jsou například FTP, HTTP, SMTP, SSH, Telnet.
- 5) Každá aplikace má specifické nároky na transportní protokoly. Protokol UDP je jednoduchý protokol, který se hodí všude tam, kde není až tak kritická ztráta nějakého paketu, ale je důležitá nízká hodnota zpoždění a kolísání zpoždění. Právě takové požadavky mají hlasové aplikace. Při přenosu souboru pomocí FTP protokolu, je naopak důležité doručení

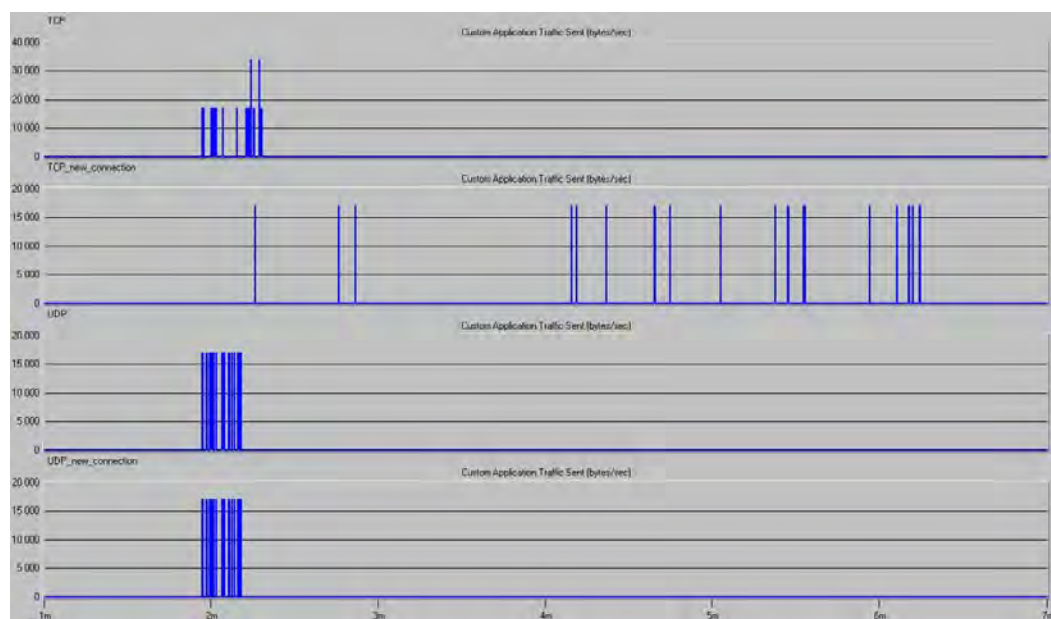
každého paketu, proto se využívá potvrzovaného transportního protokolu TCP.

## A.2 Úkol 2

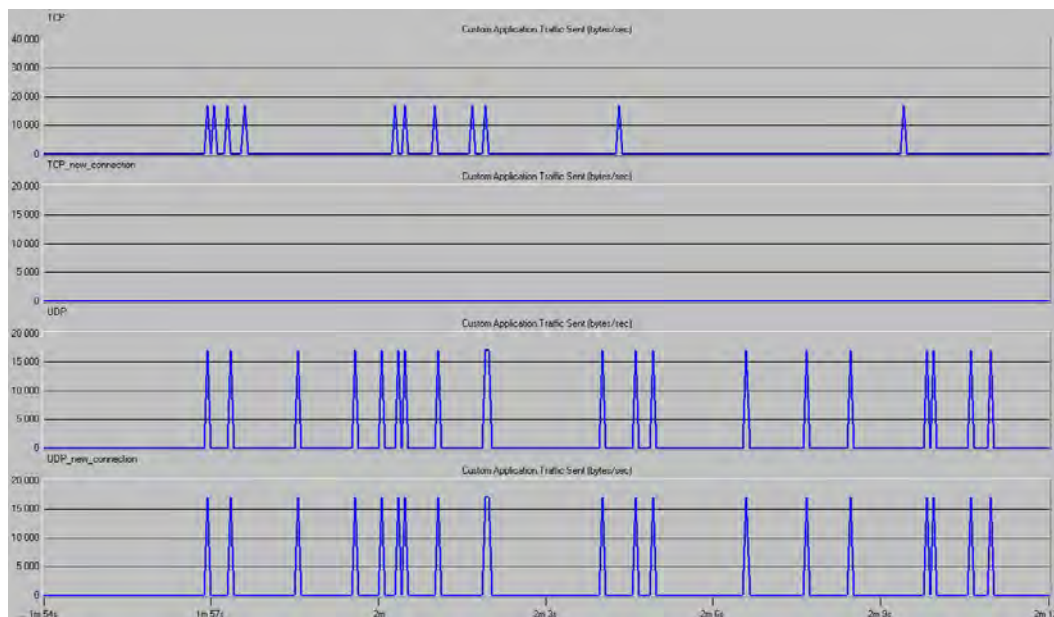
V druhé části se vytvářejí dva nové scénáře, v kterých je nastaveno navazování spojení při každém jednotlivém přenosu dat.

Doplňující otázky a úkoly:

- 1) Po simulování nových scénářů je vhodné prostudovat zejména změny oproti scénářům původním. Na konkrétní statistiky jsou zaměřeny otázky a úkoly následující.
- 2) Na obrázcích A.2 a A.3 jsou zobrazeny výsledné statistiky pro odeslaná data vytvořeným vlastním síťovým provozem. Na prvním obrázku je celková statistika, na druhém pak výřez pro určitou časovou oblast, aby bylo možné pozorovat shodnost UDP provozu v obou scénářích. Ze statistik je tedy patrné, že zatímco u UDP scénáře nedošlo k žádnému prodloužení doby přenosu, u TCP protokolu je prodloužení výrazné, což je dáno navazováním spojení před každým dílčím přenosem. Protokol UDP takový mechanismus nemá, proto doba přenosu zůstala shodná.

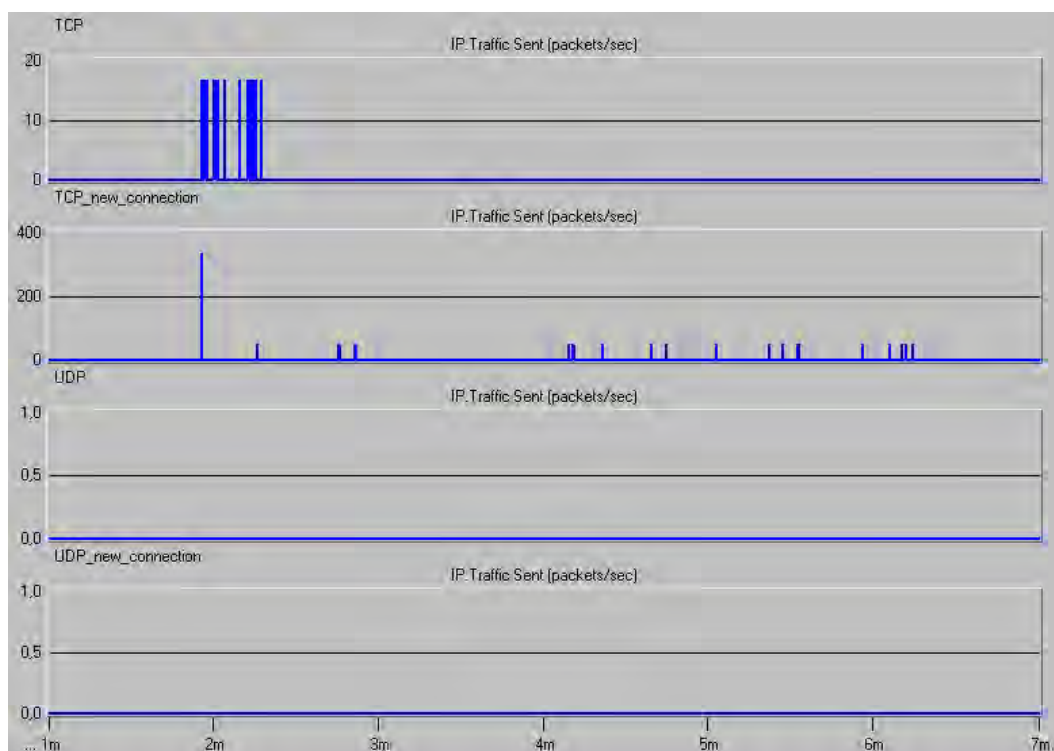


Obr. A.2: Statistika pro odeslaná data vlastní vytvořenou aplikací v bajtech/s.



Obr. A.3: Přiblížení statistiky pro odeslaná data vlastní vytvořenou aplikací v bajtech/s.

- 3) Na obrázku A.4 pod odstavcem jsou patrná data odeslaná klientem v případě TCP scénářů. Jedná se o data generovaná TCP protokolem k potvrzování rámců.

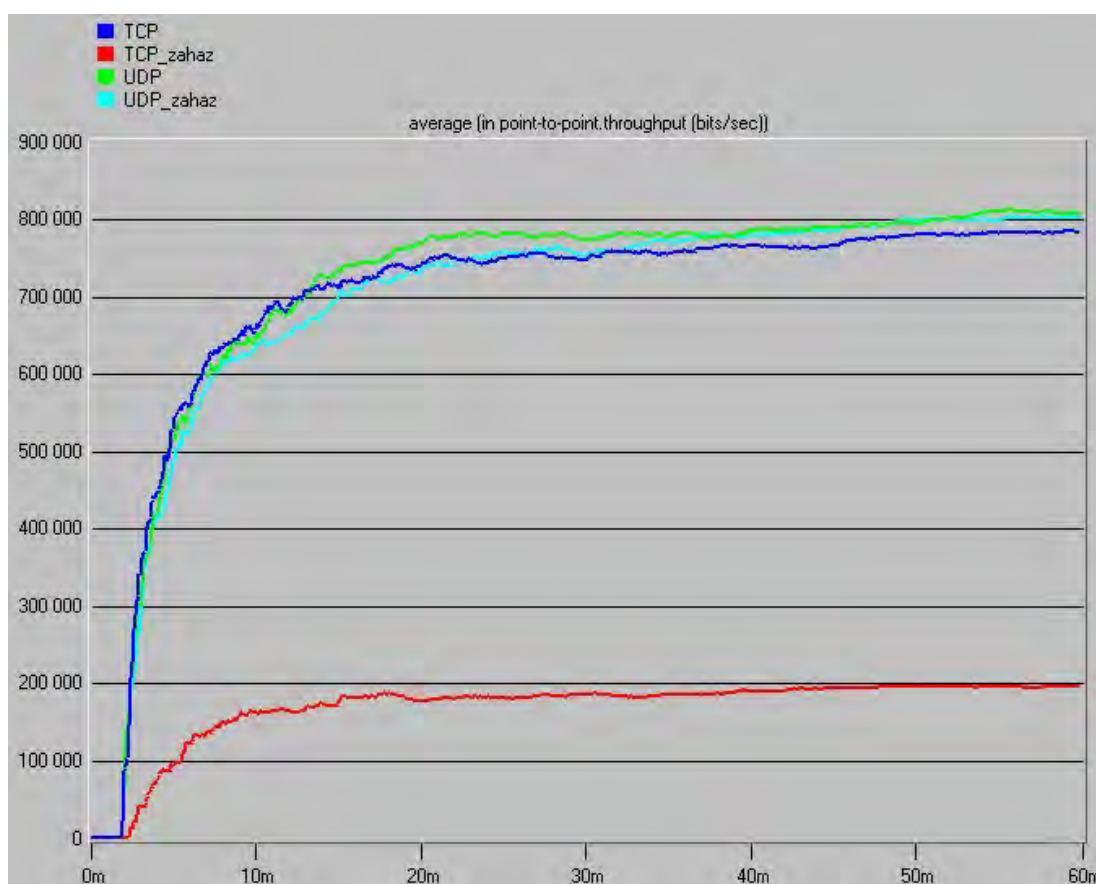


Obr. A.4: Data odeslaná klientskou podsítí v paketech/s.

### A.3 Úkol 3

Pro nové scénáře je nastaveno určité procento zahazování paketů na komponentě *IP\_cloud*.

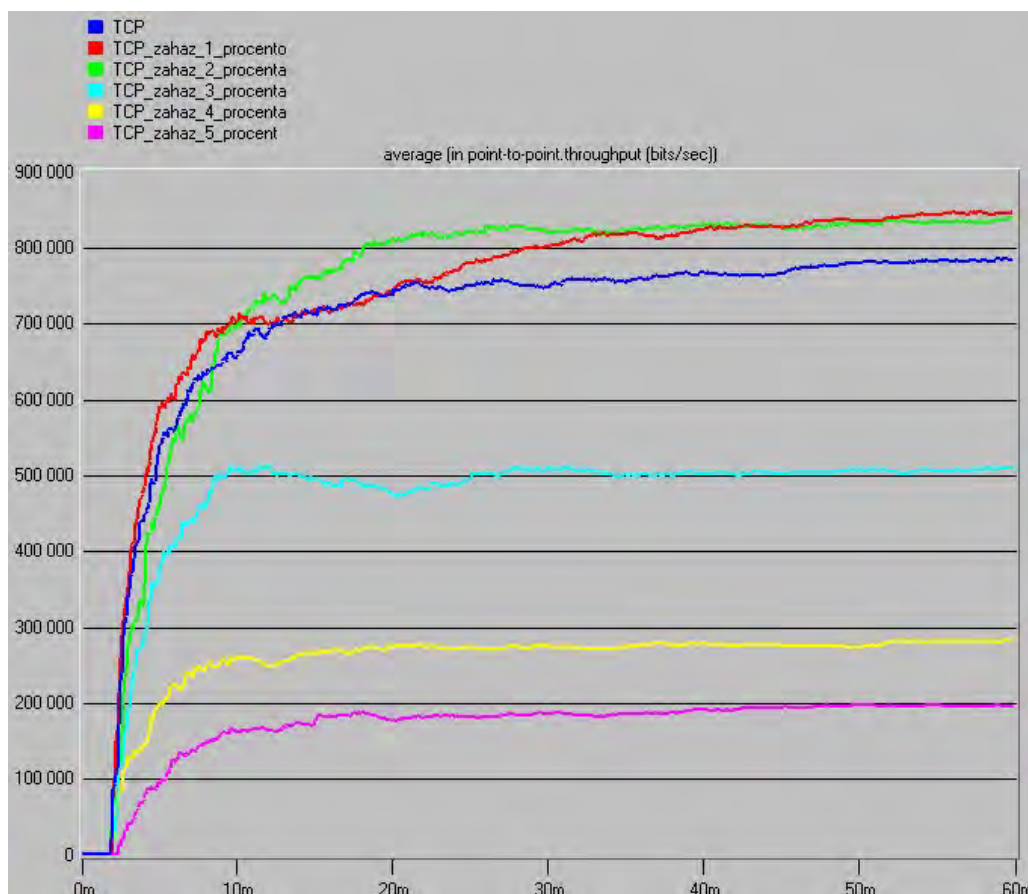
- 1) Zatímco u UDP protokolu došlo k mírnému snížení zatížení linky, u scénáře TCP při nastaveném zahazování 5 % kleslo zatížení linky přibližně na čtvrtinu původní propustnosti linky. Protokol UDP nedisponuje žádnými mechanismy pro kontrolu, či opětovné zaslání paketu při ztrátě během přenosu, proto se zatížení linky u UDP změnilo pouze o nastavené zahazování paketů, tedy poklesla o 5 %. Protokol TCP ovšem mechanismy pro zjištění ztráty paketu disponuje, proto nastalo výrazné snížení zatížení linky jako důsledek opětovného zasílání ztracených paketů. Tento fakt je možné pozorovat na obrázku A.5, kde je daná statistika znázorněna.



Obr. A.5: Zatížení linky pro scénáře UDP a TCP v bitech/s.

- 2) Na obrázku A.6 je zobrazená statistika pro různé hodnoty zahazování u TCP protokolu. Hodnoty zahazování jsou nastaveny na 0, 1, 2, 3, 4 a 5

procent. Ze statistiky je patrné, že nejnižší zatížení linky má scénář s nastaveným zahazováním 5 %. Dále lze z grafu vyčíst, že při daném síťovém provozu je protokol u scénářů s nastaveným zahazováním 1 a 2 % znovu posílat ztracené pakety, tak že to nemá dopad na přenos sníženou propustností na lince. Naopak zatížení linky u těchto dvou scénářů ještě vzrostlo o znovu zasílané pakety.



Obr. A.6: Zatížení linky pro scénáře TCP s různou hodnotou zahazování paketů v bitech/s.

## **B ŘEŠENÍ PRO SROVNÁNÍ WLAN S ETHERNETEM**

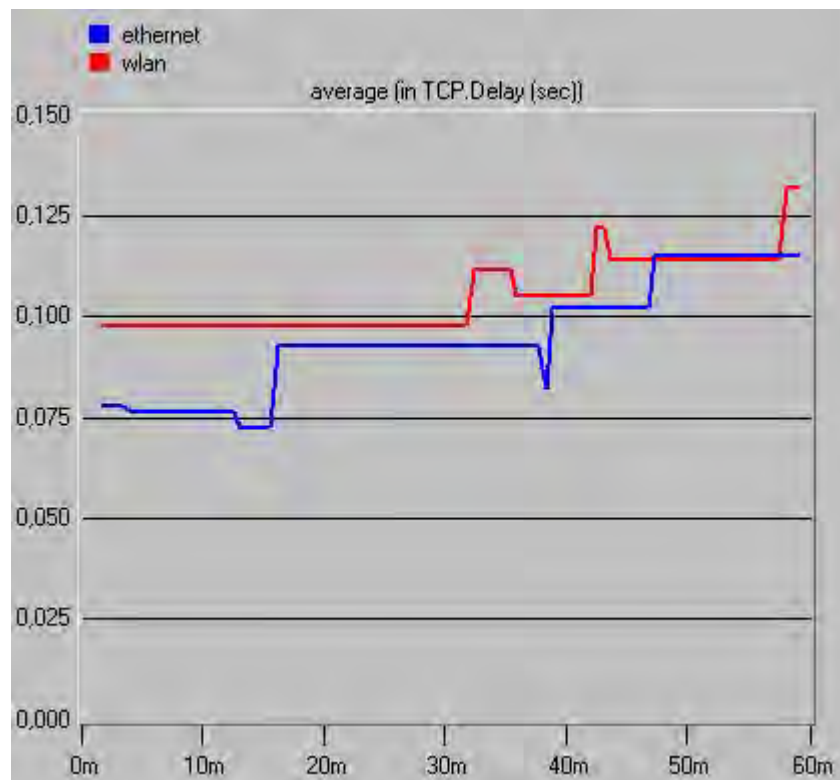
Laboratorní úloha se zabývá porovnáním přenosových parametrů sítě v závislosti na použité přenosové technologii. Jako zástupce klasických drátových technologií je použit nejrozšířenější protokol u LAN sítí Ethernet (ve variantě 10BaseT) a jeho parametry jsou srovnávány s bezdrátovou technologií WLAN o rychlosti 11Mbit/s, což je maximální přenosová rychlost podporovaná programem IT Guru.

### **B.1 Úkol 1**

V tomto úkolu jsou vytvořeny 2 scénáře. V prvním scénáři se konfiguruje základní topologie k úloze a nastaví se jednotlivé parametry vytvořené aplikace FTP a zajistí se podpora na jednotlivých prvcích topologie. V druhém konfigurovaném scénáři se v klientské podsíti vytvoří bezdrátová síť tak, aby mohlo nastat porovnání mezi technologiemi Ethernet a WLAN.

Doplňující otázky a úkoly:

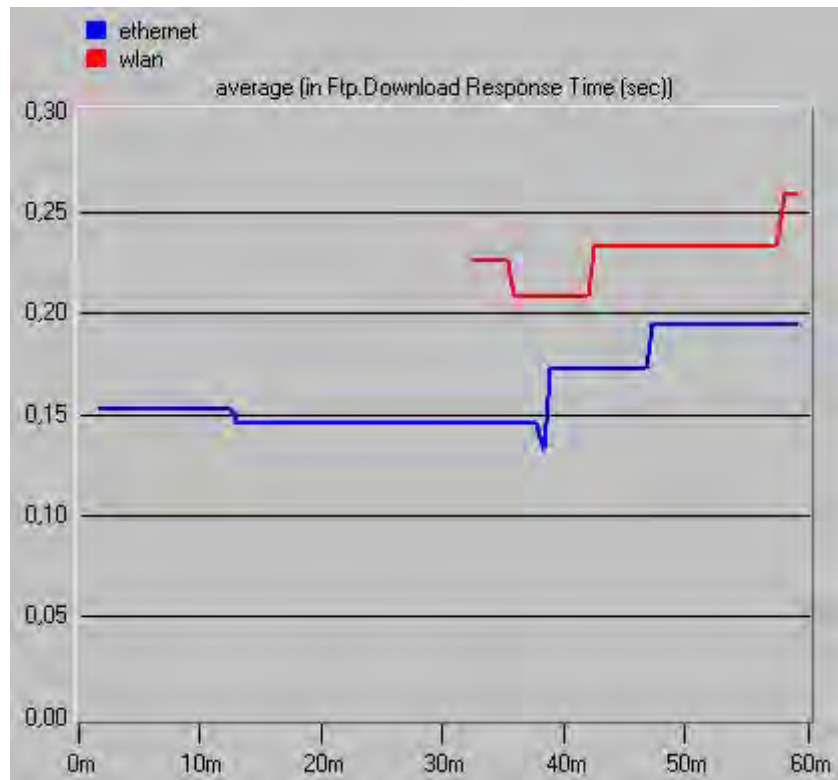
- 1) Jednotlivé simulované statistiky je možné si prohlédnout podle pokynů v prvním doplňujícím úkolu této úlohy.
- 2) Graf pro celkové TCP zpoždění v síti je na obrázku B.1. Z grafu je patrné, že celkové průměrné zpoždění u scénáře s bezdrátovým přenosem nabývá vyšších hodnot, což je způsobené specifikacemi bezdrátových sítí.



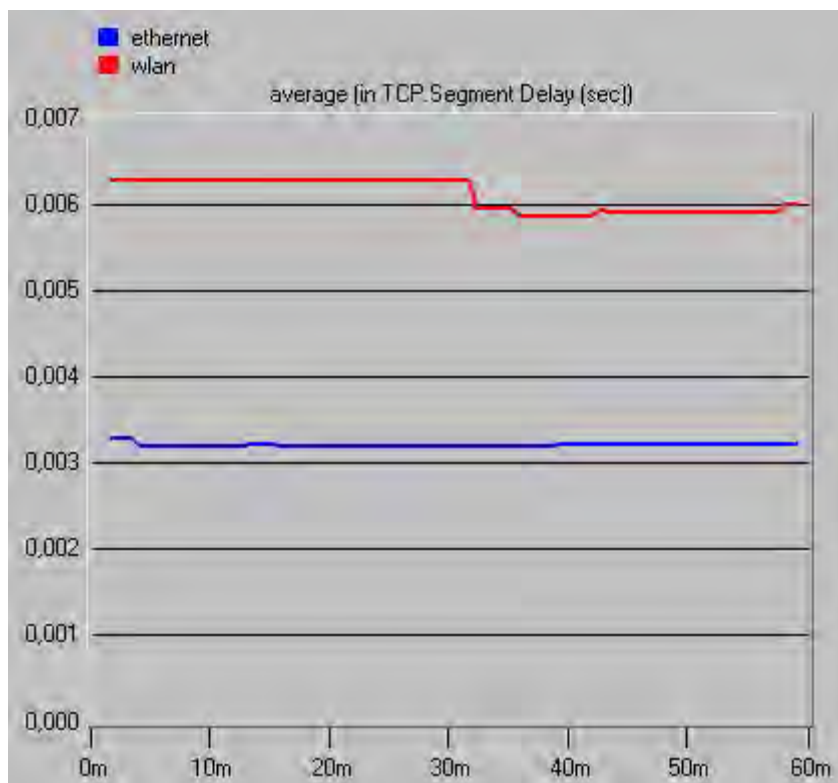
Obr. B.1: Porovnání celkového zpoždění u TCP provozu v s/min.

- 3) Rozdíly mezi jednotlivými přenosovými technologiemi lze pozorovat například v grafu *Global Statistics/FTP/Download response Time (sec)* (Obr. B.2), u kterého je možné pozorovat delší dobu odezvy u scénáře WLAN. Křivka pro tento scénář není vykreslena přes celý graf, což je způsobeno odesláním FTP dat v rozdílných časech simulace oproti scénáři s Ethernetem. Druhý graf ukazující rozdíly mezi technologiemi je graf *Global Statistics/TCP/Segment Delay (sec)* (Obr. B.3), který znázorňuje zpoždění pro TCP provoz.





Obr. B.2: Doba odezvy pro FTP data v síti v s/min.



Obr. B.3: Zpoždění pro celkové TCP data v síti v s/min.



## B.2 Úkol 2

V druhém úkolu této úlohy probíhá konfigurace nových scénářů a přenastavení prvků topologie pro podporu VoIP aplikace, která slouží k ověření závislosti hlasových služeb na vzdálenosti bezdrátového klienta a porovnání s technologií ethernet.

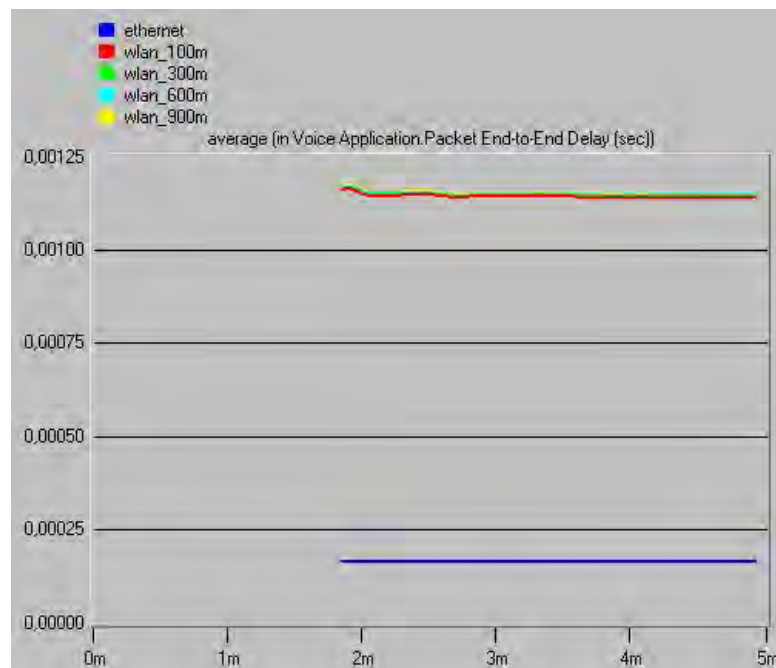
Doplňující otázky a úkoly:

- 1) Ze zjištěných závislostí vyplývá, že s rostoucí vzdáleností bezdrátového klienta od přístupového bodu roste zpoždění hlasových služeb. Zpoždění u bezdrátového klienta je oproti ethernetovému klientovi přibližně pětkrát větší.
- 2) Po vytvoření nových scénářů a nastavení různých vzdáleností klienta od přístupového bodu lze vyvodit závěr, že maximální komunikační dosah bezdrátového klienta je v tomto případě přibližně 1200m. Na obrázku B.4 je ukázka nastavení vzdálenosti 1200m mezi přístupovým bodem a klientem.

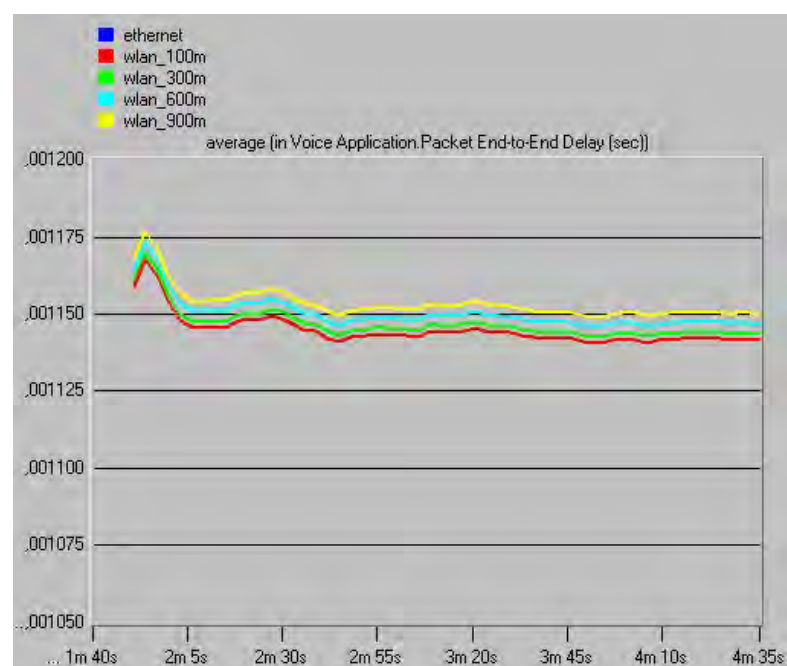


Obr. B.4: Nastavení vzdálenosti bezdrátového klienta do vzdálenosti 1200m od přístupového bodu.

- 3) Na obrázku B.5 a B.6 je možné pozorovat vliv vzdálenosti klienta od přístupového bodu na přenosových parametrech, konkrétně na zpoždění od serveru ke klientovi. První obrázek ukazuje celkový přehled včetně křivky pro Ethernet. V následujícím obrázku je aplikován výřez pro názornější ukázkou rostoucího zpoždění u bezdrátového klienta na vzdálenosti.



Obr. B.5: Zpoždění hlasové aplikace pro různé hodnoty vzdálenosti bezdrátového klienta od přístupového bodu v s/min.



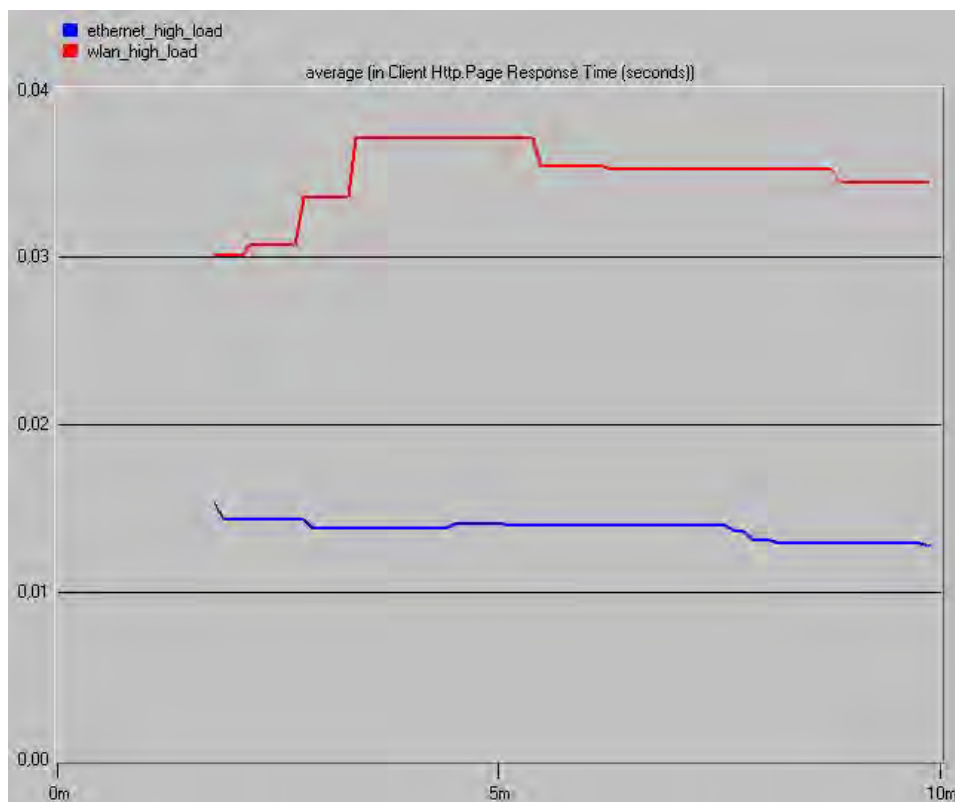
Obr. B.6: Přiblížení statistiky pro zpoždění hlasové aplikace pro různé hodnoty vzdálenosti bezdrátového klienta od přístupového bodu v s/min.

## B.3 Úkol 3

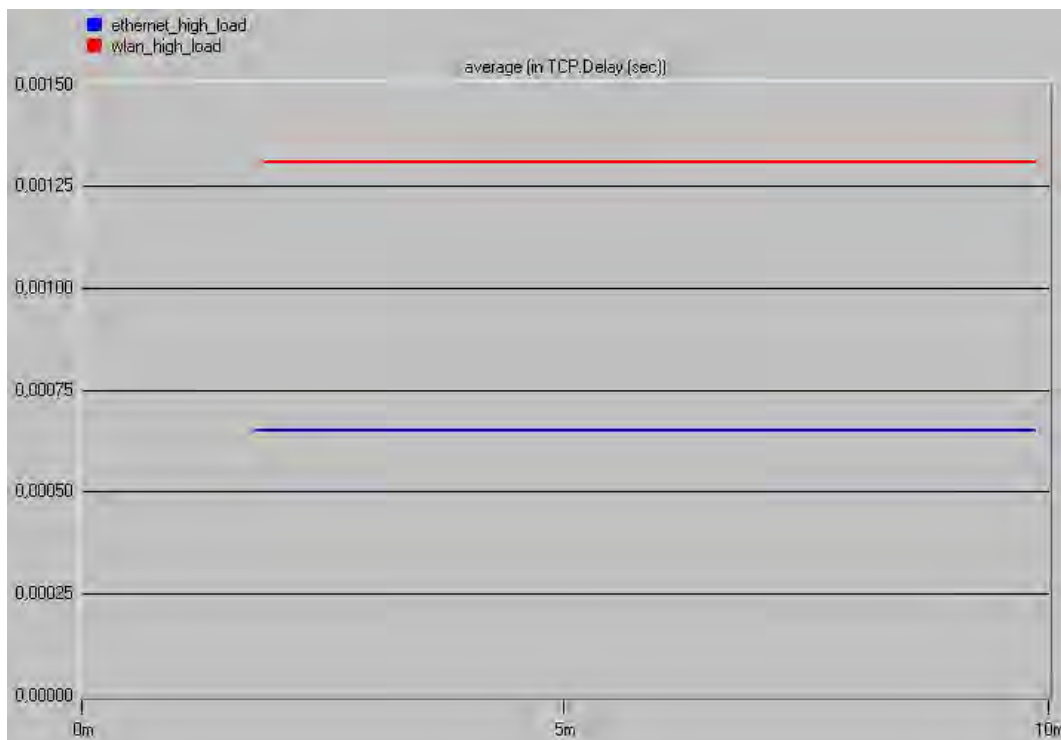
Třetí úkol je zaměřen na porovnání přenosových technologií v případě většího síťového provozu. Topologie proto byla rozšířena o nové servery a klienty, na kterých byly nakonfigurovány odlišné aplikace FTP, HTTP a voice.

Doplňující otázky a úkoly:

- 1) U http klienta byla vybrána statistika *Page Response Time (seconds)* (Obr. B.7) znázorňující delší dobu odezvy u wlan scénáře. V případě FTP klienta byla vybrána statistika *TCP/Delay (seconds)* (Obr. B.8), v které je možné pozorovat přibližně dvojnásobné zpoždění v případě bezdrátového klienta.

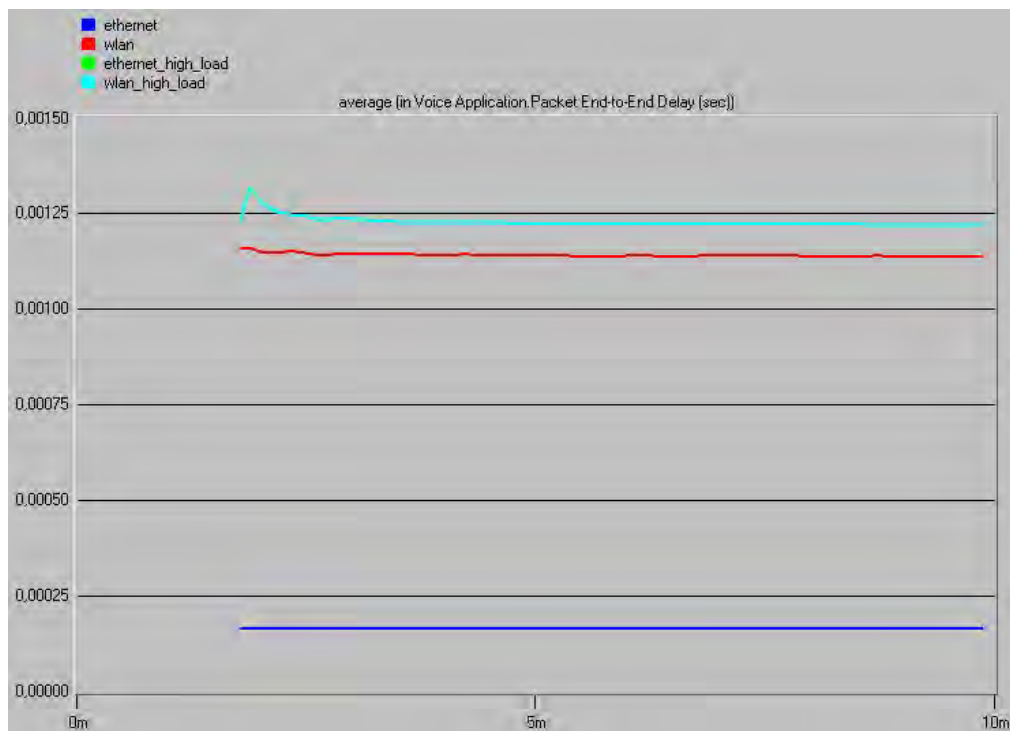


Obr. B.7: Odezva HTTP serveru v s/min.

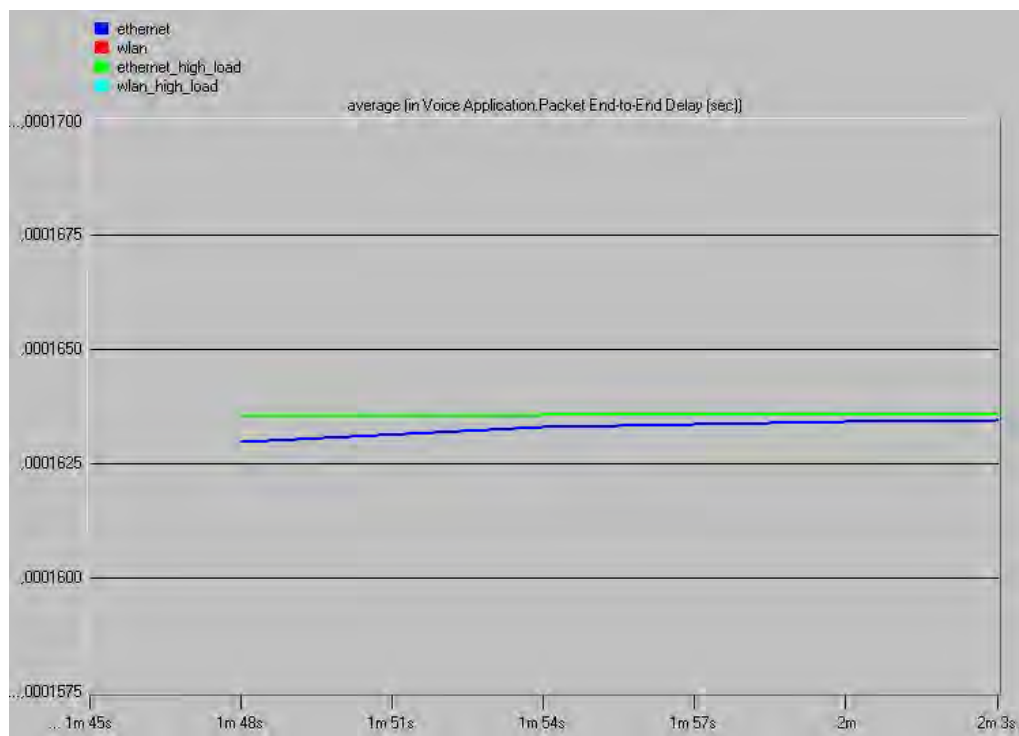


Obr. B.8: Průměrné zpoždění pro TCP spojení na FTP klientu v s/min.

- 2) Graf pro dané statistiky je možné si prohlédnout na obrázku B.9 a B.10 pod textem. Z uvedených grafů je patrné, že zatímco u bezdrátové sítě WLAN dochází k nárůstu zpoždění při zvýšené zátěži na síti, u technologie Ethernet je zvýšení patrné až ve výřezu a přiblížení této statistiky na obrázku následujícím.



Obr. B.9: Zpoždění hlasové aplikace na klientovi pro odlišný typ zátěže v síti v s/min.



Obr. B.10: Přiblížení statistiky pro zpoždění hlasové aplikace na klientovi pro odlišný typ zátěže v síti v s/min.

## C ŘEŠENÍ PRO SMĚROVACÍ PROTOKOLY

Laboratorní úloha je zaměřena na směrovací protokoly RIP a OSPF patřící do skupiny IGP (Interior Gateway routing Protocol) protokolů.

### C.1 Úkol 1

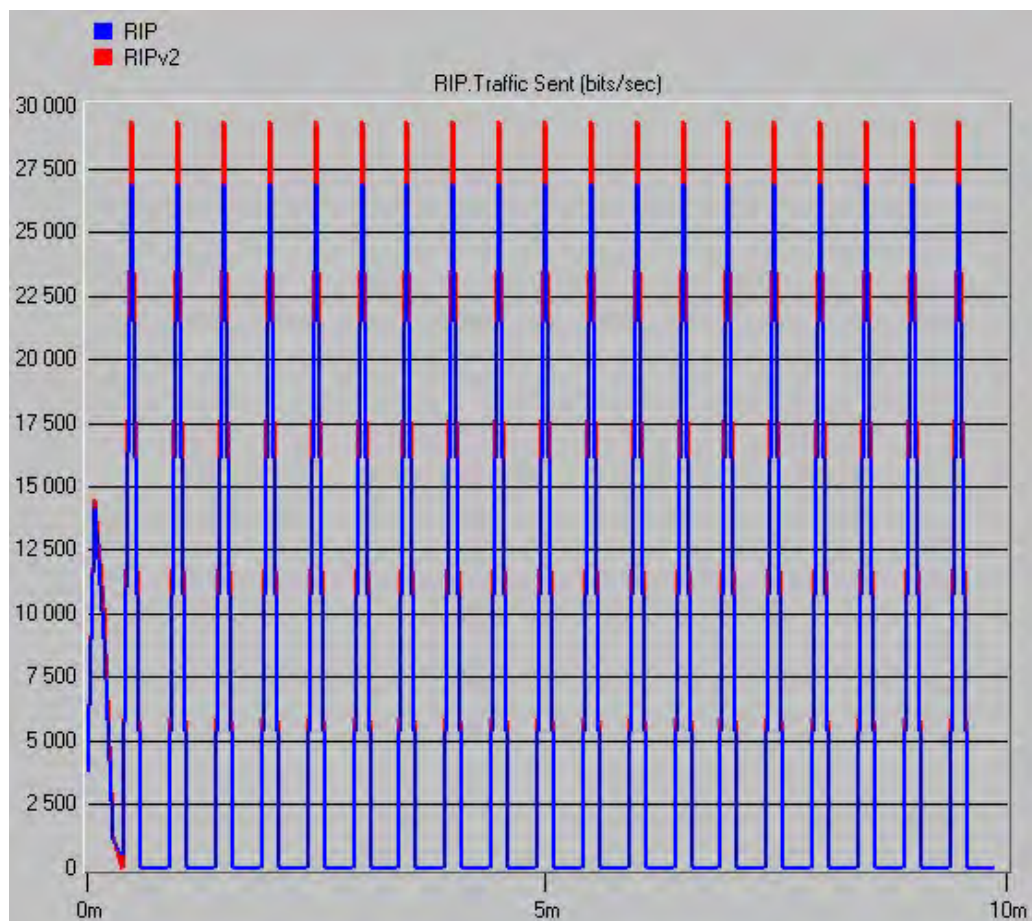
První část úlohy je zaměřena na směrovací protokol RIP, který je programem přednastaven jako výchozí směrovací protokol v jeho první verzi. V prvním scénáři je vytvořena výchozí topologie úlohy a ke směrování použit právě předkonfigurovaný protokol RIP. Pro druhý scénář tohoto úkolu byl nastaven směrovací protokol RIPv2.

Doplňující otázky a úkoly:

- 1) U první verze protokolu RIP aktualizace směrovacích tabulek neobsahují záznamy o masce dané sítě. Proto nepřipadá v úvahu používání beztřídního adresování u této verze protokolu RIP. V síti by nastaly problémy s doručení paketů, protože by směrovače měly ve směrovacích tabulkách shodné informace pro více podsítí.
- 2) Sumarizaci IP adres je nutné vypnout u druhé verze RIP protokolu opět z důvodu použití beztřídního adresování.
- 3) První verze RIP protokolu šíří směrovací informace všesměrovým vysíláním (broadcast) a jelikož prvek „100BaseT\_LAN“, který simuluje LAN síť, nenaslouchá na portu 520, který je určen právě pro RIP protokol, dané datagramy zahazuje. U druhé verze protokolu RIP je zasílání aktualizací informací řešeno skupinovým vysíláním (multicast).
- 4) V simulované topologii je 14 dvoubodových spojů, přičemž každý dvoubodový spoj potřebuje adresní prostor s prefixem /30. V každé podsíti je simulována LAN síť s 10 PC a jedním serverem. Potřebuje tedy adresní prostor s prefixem /28, v kterém je možné využít 14 IP adres pro adresaci koncových zařízení. Celkově je pro danou topologii třeba:
  - 14 x adresa s prefixem /30, v které je možné využít 2 (4-2) adresy pro adresaci koncových zařízení,
  - 3 x adresa s prefixem /28, v které je možné využít 14 (16-2) adres

pro adresaci koncových zařízení.

- 5) Adresy 10.10.10.0/24 a 10.10.20.0/24 patří mezi neveřejné adresy třídy A.  
Adresy 150.10.10.0/24 a 150.10.20.0/24 patří mezi veřejné adresy třídy B.  
Adresy 172.16.10.0/24 a 172.16.20.0/24 patří mezi neveřejné adresy třídy B.
- 6) Zvýšenou zátěž je možné pozorovat u scénáře s nakonfigurovanou druhou verzí protokolu RIP v důsledku obsáhlejších směrovacích tabulek, kde se přenášejí i informace o masce sítě. Statistika je znázorněna na obrázku C.1.



Obr. C.1: Celkový provoz RIP protokolu verze 1 a 2 v bitech/s.

## C.2 Úkol 2

Druhý úkol je zaměřen na směrovací protokol OSPF. Vytváří se dva nové scénáře pro simulaci OSPF protokolu s nastavenými oblastmi i bez nich.

Doplňující otázky a úkoly:



- 1) Ze směrovacích tabulek (Obr. C.2 a Obr. C.3) je patrné, že pro scénář bez rozdělení na oblasti je směrovací tabulka znatelně obsáhlejší. Obsahuje směrovací informace pro celou topologii sítě. Směrovací tabulka pro scénář s oblastmi obsahuje pouze směrovací informace pro danou oblast.

COMMON ROUTE TABLE snapshot for:

Router name: Campus Network.podsit\_Brno.Brno\_hlavni  
at time: 600,00 seconds

ROUTE TABLE contents:

Dest. Address	Subnet Mask	Next Hop	Interface Name	Metric	Protocol	Insertion Time
10.10.10.0	255.255.255.252	192.0.19.1	IF10	200	OSPF	59,179
10.10.20.0	255.255.255.252	192.0.19.1	IF10	200	OSPF	59,179
150.10.10.0	255.255.255.0	150.10.10.1	IF0	0	Direct	0,000
150.10.20.0	255.255.255.0	150.10.20.1	IF1	0	Direct	0,000
192.0.19.0	255.255.255.0	192.0.19.2	IF10	0	Direct	0,000
192.0.25.0	255.255.255.0	192.0.25.1	Loopback	0	Direct	0,000
192.0.21.0	255.255.255.0	192.0.19.1	IF10	30	OSPF	59,179
192.0.3.0	255.255.255.0	192.0.19.1	IF10	60	OSPF	59,179
192.0.20.0	255.255.255.0	192.0.19.1	IF10	60	OSPF	59,179
192.0.17.0	255.255.255.0	192.0.19.1	IF10	70	OSPF	59,179
192.0.16.0	255.255.255.0	192.0.19.1	IF10	80	OSPF	59,179
192.0.0.0	255.255.255.0	192.0.19.1	IF10	70	OSPF	59,179
192.0.14.0	255.255.255.0	192.0.19.1	IF10	80	OSPF	59,179
192.0.8.0	255.255.255.0	192.0.19.1	IF10	140	OSPF	59,179
192.0.5.0	255.255.255.0	192.0.19.1	IF10	190	OSPF	59,179
192.0.6.0	255.255.255.0	192.0.19.1	IF10	140	OSPF	59,179
192.0.7.0	255.255.255.0	192.0.19.1	IF10	170	OSPF	59,179
192.0.22.0	255.255.255.0	192.0.19.1	IF10	60	OSPF	59,179
192.0.2.0	255.255.255.0	192.0.19.1	IF10	90	OSPF	59,179
192.0.10.0	255.255.255.0	192.0.19.1	IF10	90	OSPF	59,179
192.0.9.0	255.255.255.0	192.0.19.1	IF10	90	OSPF	59,179
192.0.4.0	255.255.255.0	192.0.19.1	IF10	60	OSPF	59,179
192.0.1.0	255.255.255.0	192.0.19.1	IF10	70	OSPF	59,179
192.0.15.0	255.255.255.0	192.0.19.1	IF10	80	OSPF	59,179
192.0.13.0	255.255.255.0	192.0.19.1	IF10	80	OSPF	59,179
192.0.12.0	255.255.255.0	192.0.19.1	IF10	120	OSPF	59,179
192.0.11.0	255.255.255.0	192.0.19.1	IF10	120	OSPF	59,179
192.0.18.0	255.255.255.0	192.0.19.1	IF10	70	OSPF	59,179
192.0.23.0	255.255.255.0	192.0.19.1	IF10	190	OSPF	59,179
192.0.24.0	255.255.255.0	192.0.19.1	IF10	80	OSPF	59,179
172.16.10.0	255.255.255.0	192.0.19.1	IF10	90	OSPF	59,179
172.16.20.0	255.255.255.0	192.0.19.1	IF10	90	OSPF	59,179

The gateway of last resort is not set

Obr. C.2: Směrovací tabulka pro směrovač v podsíti Brno ve scénáři bez nakonfigurovaných oblastí.

COMMON ROUTE TABLE snapshot for:

Router name: Campus Network.podsit\_Brno.Brno\_hlavni  
at time: 600,00 seconds

ROUTE TABLE contents:

Dest. Address	Subnet Mask	Next Hop	Interface Name	Metric	Protocol	Insertion Time
150.10.10.0	255.255.255.0	150.10.10.1	IF0	0	Direct	0,000
150.10.20.0	255.255.255.0	150.10.20.1	IF1	0	Direct	0,000
192.0.19.0	255.255.255.0	192.0.19.2	IF10	0	Direct	0,000
192.0.25.0	255.255.255.0	192.0.25.1	Loopback	0	Direct	0,000
192.0.2.0	255.255.255.0	192.0.19.1	IF10	90	OSPF	59,179
192.0.3.0	255.255.255.0	192.0.19.1	IF10	60	OSPF	59,179
192.0.21.0	255.255.255.0	192.0.19.1	IF10	30	OSPF	59,179
192.0.20.0	255.255.255.0	192.0.19.1	IF10	60	OSPF	59,179
192.0.22.0	255.255.255.0	192.0.19.1	IF10	60	OSPF	59,179

The gateway of last resort is not set

Obr. C.3: Směrovací tabulka pro směrovač v podsíti Brno ve scénáři s oblastmi.

- 2) Protokol OSPF je charakteristický tím, že každý směrovač zná topologii celé sítě. Tato úvodní procedura zabere při dané topologii téměř 60 sekund, zatímco poslední záznam u RIP protokolu je pro směrovač uvnitř podsítě Brno vložen v čase 18 sekund.
- 3) Směrovací tabulka pro směrovač 6 (Obr. C.4), v které je patrná dostupnost dvou stejně ohodnocených cest pro stejnou cílovou síť, je uvedena



pod textem. Tato skutečnost může být využita pro rozdělení zátěže v síti mezi více cest.

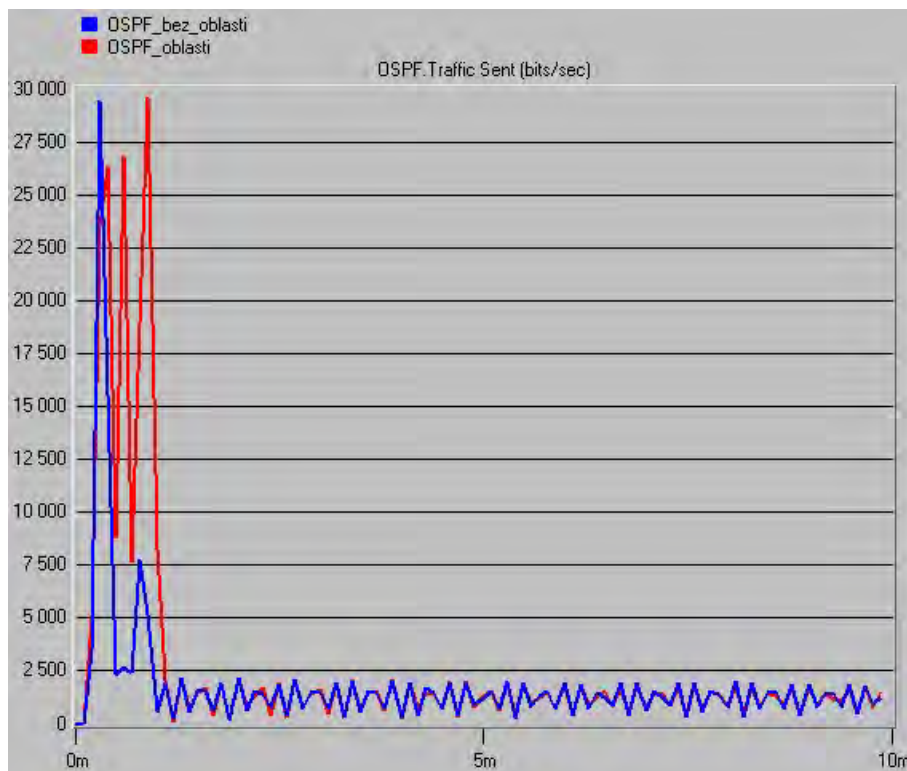
```

1  COMMON ROUTE TABLE snapshot for:
2
3  Router name: Campus Network.smerovac_6
4  at time: 600,00 seconds
5
6  ROUTE TABLE contents:
7
8  -----
9  | Dest. Address | Subnet Mask | Next Hop | Interface Name | Metric | Protocol | Insertion Time |
10 |-----|-----|-----|-----|-----|-----|-----|
11 | 10.10.10.0 | 255.255.255.252 | 192.0.13.1 | IF4 | 130 | OSPF | 57,225 |
12 | 10.10.20.0 | 255.255.255.252 | 192.0.13.1 | IF4 | 130 | OSPF | 57,225 |
13 | 192.0.13.0 | 255.255.255.0 | 192.0.13.2 | IF4 | 0 | Direct | 0,000 |
14 | 192.0.11.0 | 255.255.255.0 | 192.0.11.2 | IF10 | 0 | Direct | 0,000 |
15 | 192.0.1.0 | 255.255.255.0 | 192.0.1.2 | IF11 | 0 | Direct | 0,000 |
16 | 192.0.18.0 | 255.255.255.0 | 192.0.18.1 | Loopback | 0 | Direct | 0,000 |
17 | 192.0.21.0 | 255.255.255.0 | 192.0.1.1 | IF11 | 40 | OSPF | 57,225 |
18 | 192.0.19.0 | 255.255.255.0 | 192.0.1.1 | IF11 | 70 | OSPF | 57,225 |
19 | 192.0.3.0 | 255.255.255.0 | 192.0.1.1 | IF11 | 40 | OSPF | 57,225 |
20 | 192.0.20.0 | 255.255.255.0 | 192.0.1.1 | IF11 | 70 | OSPF | 57,225 |
21 | 192.0.17.0 | 255.255.255.0 | 192.0.1.1 | IF11 | 20 | OSPF | 57,225 |
22 | 192.0.16.0 | 255.255.255.0 | 192.0.13.1 | IF4 | 20 | OSPF | 57,225 |
23 | 192.0.13.1 | 255.255.255.0 | 192.0.1.1 | IF11 | 30 | OSPF | 57,225 |
24 | 192.0.0.0 | 255.255.255.0 | 192.0.1.1 | IF4 | 30 | OSPF | 57,225 |
25 | 192.0.14.0 | 255.255.255.0 | 192.0.1.1 | IF11 | 20 | OSPF | 57,225 |
26 | 192.0.8.0 | 255.255.255.0 | 192.0.13.1 | IF4 | 20 | OSPF | 57,225 |
27 | 192.0.5.0 | 255.255.255.0 | 192.0.13.1 | IF4 | 70 | OSPF | 57,225 |
28 | 192.0.6.0 | 255.255.255.0 | 192.0.13.1 | IF4 | 120 | OSPF | 57,225 |
29 | 192.0.7.0 | 255.255.255.0 | 192.0.13.1 | IF4 | 70 | OSPF | 57,225 |
30 | 192.0.22.0 | 255.255.255.0 | 192.0.11.1 | IF10 | 100 | OSPF | 57,225 |
31 | 192.0.2.0 | 255.255.255.0 | 192.0.1.1 | IF11 | 40 | OSPF | 57,225 |
32 | 192.0.10.0 | 255.255.255.0 | 192.0.1.1 | IF11 | 40 | OSPF | 57,225 |
33 | 192.0.9.0 | 255.255.255.0 | 192.0.13.1 | IF4 | 20 | OSPF | 57,225 |
34 | 192.0.15.0 | 255.255.255.0 | 192.0.13.1 | IF4 | 20 | OSPF | 57,225 |
35 | 192.0.4.0 | 255.255.255.0 | 192.0.1.1 | IF11 | 10 | OSPF | 57,225 |
36 | 192.0.12.0 | 255.255.255.0 | 192.0.11.1 | IF10 | 50 | OSPF | 57,225 |
37 | 192.0.23.0 | 255.255.255.0 | 192.0.13.1 | IF4 | 120 | OSPF | 57,225 |
38 | 192.0.24.0 | 255.255.255.0 | 192.0.1.1 | IF11 | 30 | OSPF | 57,225 |
39 | 172.16.10.0 | 255.255.255.0 | 192.0.13.1 | IF4 | 30 | OSPF | 57,225 |
40 | 172.16.20.0 | 255.255.255.0 | 192.0.1.1 | IF11 | 40 | OSPF | 57,225 |
41 | 192.0.25.0 | 255.255.255.0 | 192.0.1.1 | IF11 | 40 | OSPF | 57,225 |
42 | 150.10.10.0 | 255.255.255.0 | 192.0.1.1 | IF4 | 40 | OSPF | 57,225 |
43 | 150.10.20.0 | 255.255.255.0 | 192.0.1.1 | IF11 | 40 | OSPF | 57,225 |
44 | 150.10.10.0 | 255.255.255.0 | 192.0.1.1 | IF11 | 80 | OSPF | 57,225 |
45 | 150.10.20.0 | 255.255.255.0 | 192.0.1.1 | IF11 | 80 | OSPF | 57,225 |
46
47

```

Obr. C.4: Směrovací tabulka pro směrovač\_6.

- 4) Zvýšenou zátěž je možné pozorovat pro scénář, kde je topologie rozdělena na oblasti, viz Obr. C.5. Zvýšená zátěž je dána vlastnostmi OSPF protokolu, kdy se v každé oblasti zvlášť počítá SPF algoritmus pro všechny oblasti a také se směrovací informace pro celou topologii musí přeposlat hraničním směrovačům mezi oblastmi.



Obr. C.5: Celkový OSPF provoz v síti v bitech/s.

- 5) Ze získaných statistik je patrné, že protokol RIP zatěžuje síť více svými periodickými aktualizacemi. Otázka vhodnosti směrovacího protokolu pro síť s častými změnami je diskutabilní. Záleželo by na rozsáhlosti sítě a četnosti změn v síti. Obecně lze ale říci, že pro síť s velmi častými změnami v topologii je vhodnější protokol RIP, jelikož není tolik náročný na výpočetní výkon směrovačů jako protokol OSPF.
- 6) Ze zobrazeného výpisu cest lze vyčíst, že u scénáře bez oblastí (Obr. C.6) prochází nakonfigurovaný IP provoz přes více směrovačů z důvodu nejnižší celkové metriky (50+10+10). U scénáře s oblastmi (Obr. C.7) již IP provoz zůstává v dané oblasti 0.0.0.1, i přes horší celkovou metriku spoje (50+50). Protokol OSPF tedy upřednostňuje provoz v rámci dané oblasti, až poté hledí na přiřazené metriky.

Path #1

```
smerovac_6 -> smerovac_1          Campus Network.smerovac_6
Campus Network.smerovac_5 <-> smerovac_6  Campus Network.smerovac_5
Campus Network.smerovac_1 <-> smerovac_5  Campus Network.smerovac_1
```

Obr. C.6: Výpis cesty IP provozu pro scénář bez oblastí.

Path #1

```
smerovac_6 -> smerovac_1          Campus Network.smerovac_6
Campus Network.smerovac_6 <-> smerovac_3  Campus Network.smerovac_3
Campus Network.smerovac_3 <-> smerovac_2  Campus Network.smerovac_2
Campus Network.smerovac_2 <-> smerovac_1  Campus Network.smerovac_1
```

Obr. C.7: Výpis cesty IP provozu pro scénář s oblastmi.

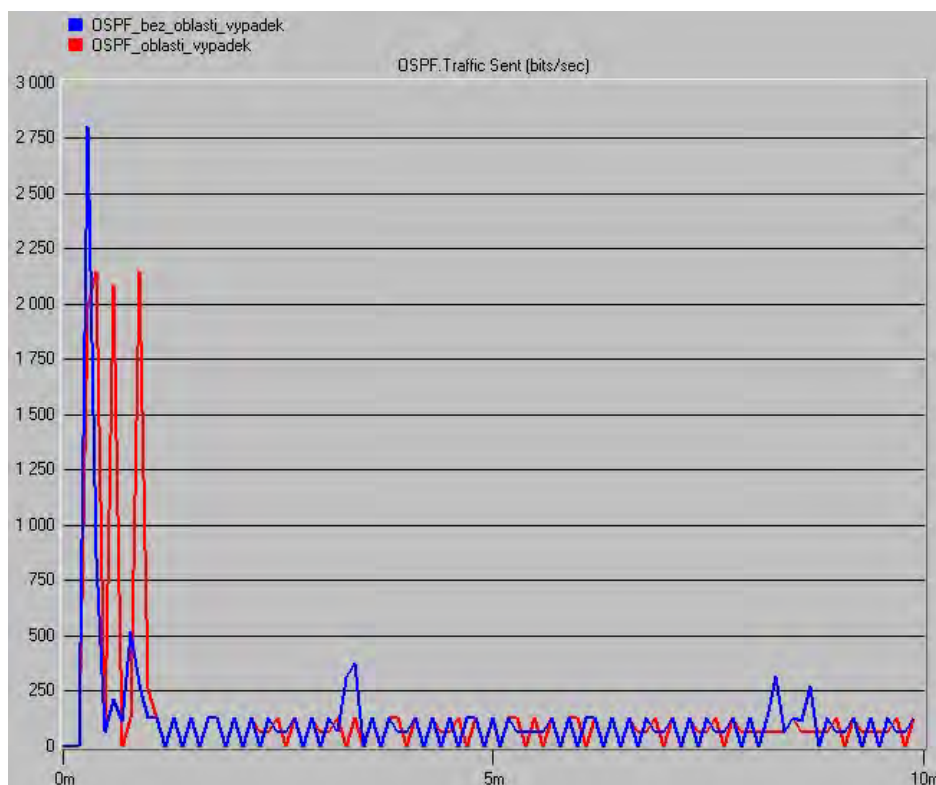
### C.3 Úkol 3

Poslední úkol této úlohy je zaměřen na chování protokolu OSPF v případě výpadku linky. Výpadek linky mezi směrovači 1 a 2 je simulován pro oba OSPF scénáře.

Doplňující otázky a úkoly:

- 1) Po prohlédnutí směrovacích tabulek pro směrovač uvnitř podsítě Brno je možné vyvodit závěr, že pro scénář bez definovaných oblastí jsou po výpadku linky přepočítány metriky pro ty cílové sítě, které tato skutečnost ovlivnila. Po opětovném obnovení linky jsou metriky opět přepočítány na původní hodnoty. Pro scénář s OSPF oblastmi výpadek linky mezi směrovači 1 a 2 směrovací tabulky na daném směrovači vůbec neovlivní, jelikož leží v jiné OSPF oblasti a má směrovací informace týkající se pouze dané oblasti.
- 2) Ze směrovacích tabulek lze vyčíst, že přepočítání směrovacích tabulek v případě výpadku linky trvá 7 sekund a přepočítání směrovacích tabulek při obnově linky 27 sekund. U směrovacího protokolu RIP by se skutečnost výpadku či obnovy projevila v periodických aktualizacích, které se posílají každých 30 sekund.
- 3) Statistika *Global Statistics/OSPF/Traffic Sent* (Obr. C.8) ukazuje celkové zatížení sítě pro OSPF provoz. Rozdělení na oblasti je však v tomto případě

vhodné zejména kvůli faktu, že se výpadek linky neprojeví zvýšeným OSPF provozem mimo danou oblast, což dokazuje následující obrázek, kde je znázorněn OSPF provoz na směrovači 9. Tento směrovač leží mimo oblast, v které došlo k výpadku linky. Modrá křivka představuje OSPF provoz scénáře bez oblastí, červená křivka provoz s oblastmi.



Obr. C.8: Celkový OSPF provoz pro scénáře s výpadkem linky v bitech/s.

## D TECHNOLOGIE ATM A FRAME RELAY

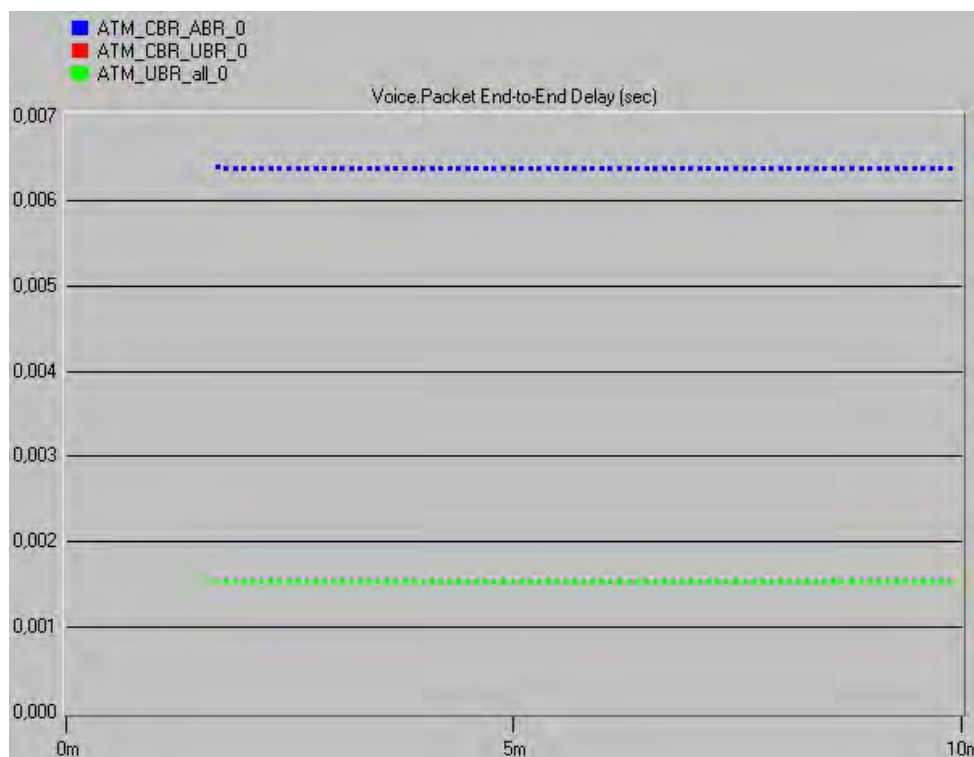
Laboratorní úloha je zaměřena na technologie pro sítě typu WAN, což jsou rozsáhlé sítě s dosahem stovky až tisíce kilometrů. Technologie ATM je univerzální přenosová technologie s pevnou délkou buňky 53 bajtů. Technologie Frame Relay poskytuje spojově orientovanou komunikaci s přepojováním paketů.

### D.1 Úkol 1

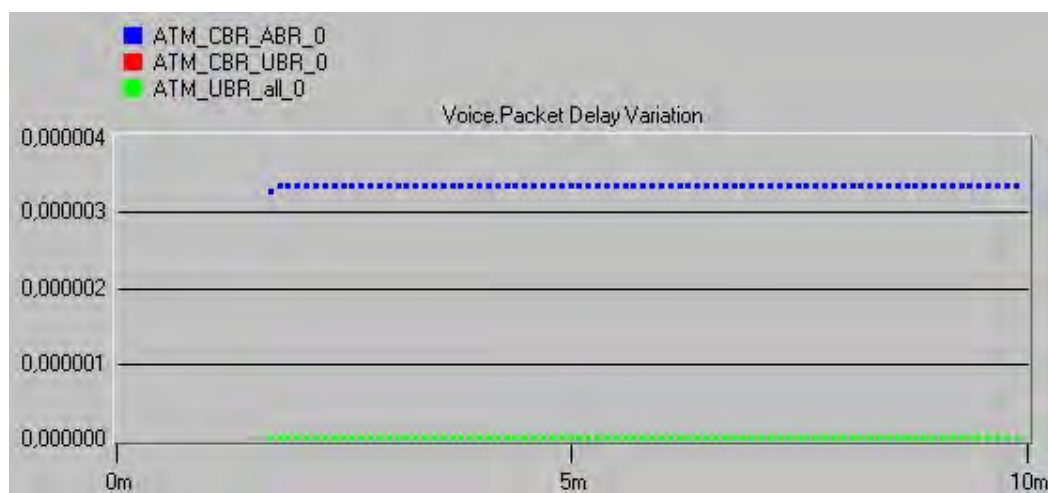
První část úlohy je zaměřena na technologii ATM. V úvodním scénáři je vytvořena základní topologie úlohy, která je postupně rozšiřována o nové scénáře s odlišným nastavením tříd služeb a provozem na pozadí.

Doplňující otázky a úkoly:

- 1) Statistika *Global Statistic/Voice/Packet End-to-End Delay (sec)* pro úvodní tři scénáře je zobrazena na obrázku D.1. Ze statistiky je patrné, že pro scénáře „ATM\_CBR\_UBR\_0“ a „ATM\_CBR\_ABR\_0“ jsou výsledky totožné (tj. křivky se překrývají), což je způsobeno charakteristikou daných tříd služeb a malým vytížením sítě, kde se neprojeví rozdíly mezi těmito třídami. Dále je možné ze statistiky pozorovat, že při nastavené třídě služeb UBR pro hlasovou aplikaci má pro tento případ příznivější statistiku v podobě menšího zpoždění a kolísání zpoždění (Obr. D.2), než při nastavené třídě služeb CBR, která je pro přenos hlasu primárně určena. Tento jev je opět způsobený nízkým zatížením sítě a faktem, že třída služeb UBR poskytuje nespojované a nesynchronizované služby. Pro statistiku na obrázku D.2 opět platí, že se křivky pro scénáře „ATM\_CBR\_UBR\_0“ a „ATM\_CBR\_ABR\_0“ překrývají, jelikož pro danou topologii sítě mají shodnou charakteristiku.

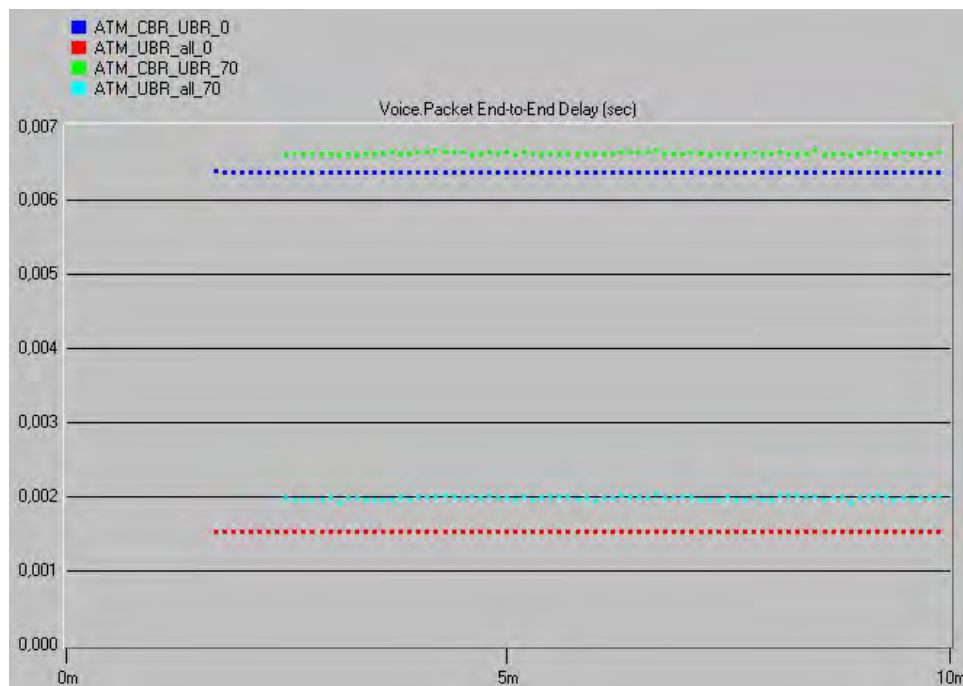


Obr. D.1: Zpoždění pro hlasovou aplikaci v úvodních scénářích v s/min.



Obr. D.2: Kolísání zpoždění pro hlasovou aplikaci v úvodních scénářích v s/min.

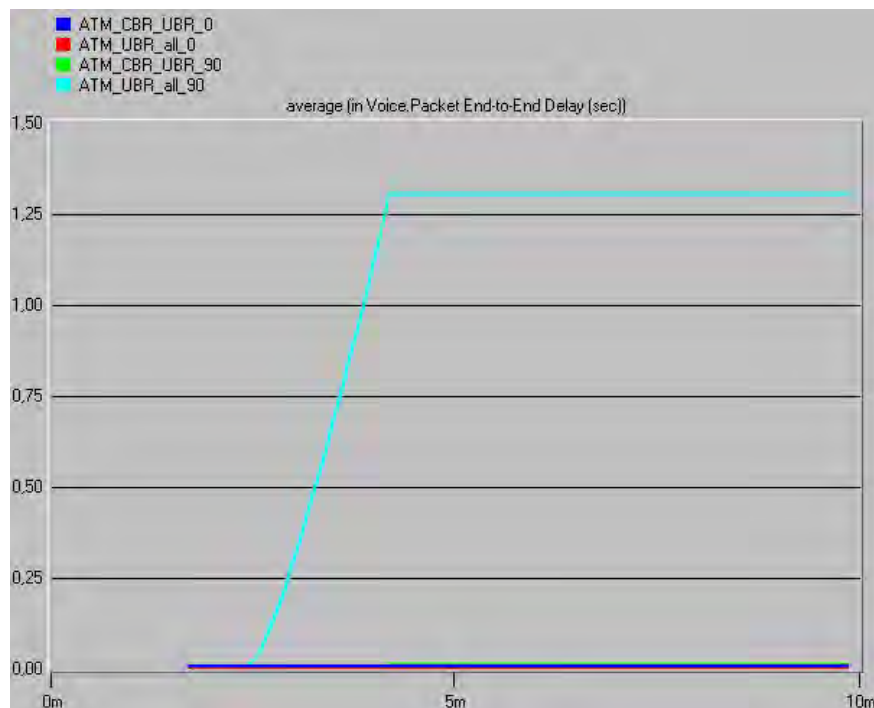
- 2) Nastavení provozu na pozadí na 70 % se u obou scénářů projeví zvýšenou hodnotou zpoždění u hlasové aplikace, viz Obr. D.3.



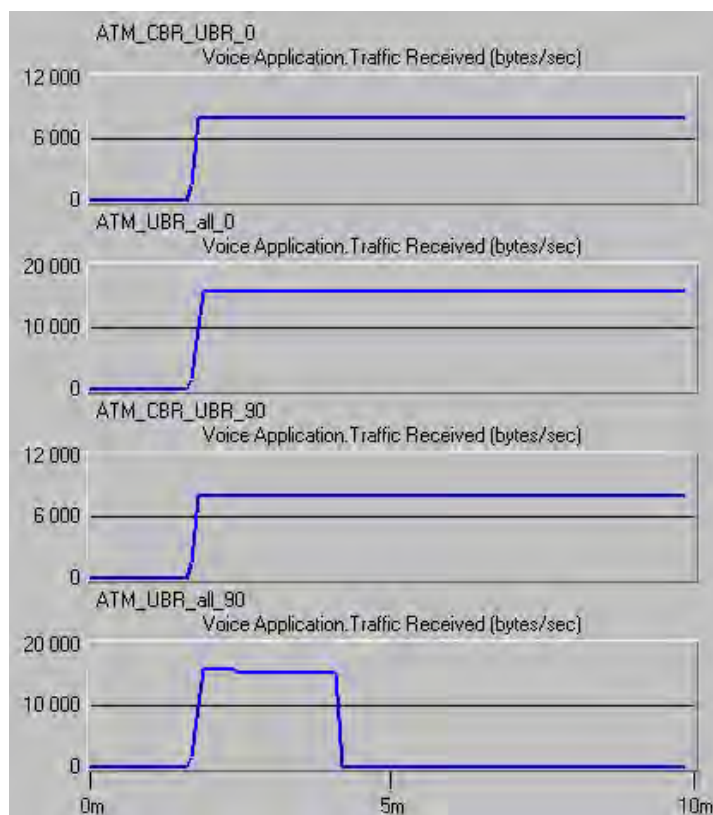
Obr. D.3: Zpoždění pro hlasovou aplikaci pro scénáře s nulovým a zvýšeným provozem na pozadí na 70 % v s/min.

- 3) U scénáře s nastavenou třídou služeb UBR pro všechny aplikace, se nastavení provozu na pozadí na hodnotu 90 % projeví růstem hodnoty zpoždění pro hlasovou aplikaci (Obr. D.4) a v důsledku zahlcení síťových prostředků přestane fungovat komunikace pro všechny ostatní aplikace v tomto scénáři (Obr. D.5). U scénáře s nastavenou třídou CBR pro hlasovou aplikaci naroste zpoždění i kolísání zpoždění (Obr. D.6), ale komunikace může stále probíhat.



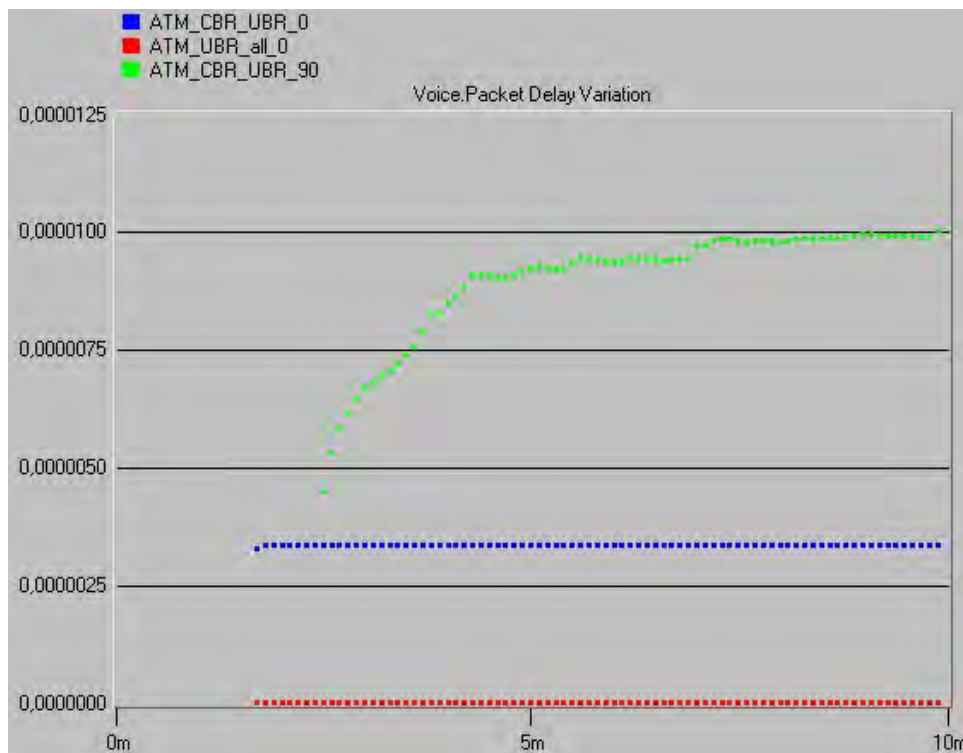


Obr. D.4: Zpoždění pro hlasovou aplikaci pro scénáře s nulovým a zvýšeným provozem na pozadí na 90 % v s/min.



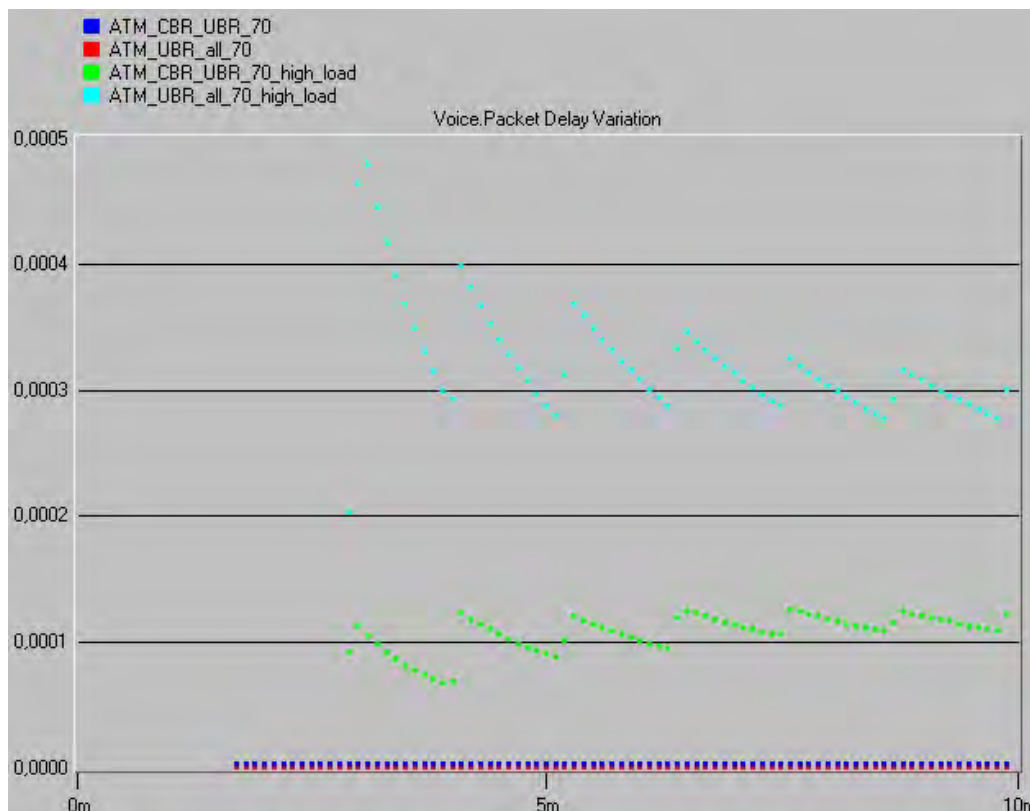
Obr. D.5: Přijatá data pro hlasovou aplikaci pro scénáře s nulovým a zvýšeným provozem na pozadí na 90 % v s/min.





Obr. D.6: Kolísání zpoždění pro hlasovou aplikaci pro scénáře s nulovým a zvýšeným provozem na pozadí na 90 % v s/min.

- 4) Zvýšená zátěž u datových aplikací má vliv na výsledné zpoždění i kolísání zpoždění pro hlasovou aplikaci (Obr. D.7) i v případě nastavené třídy služeb CBR pro hlasovou aplikaci.



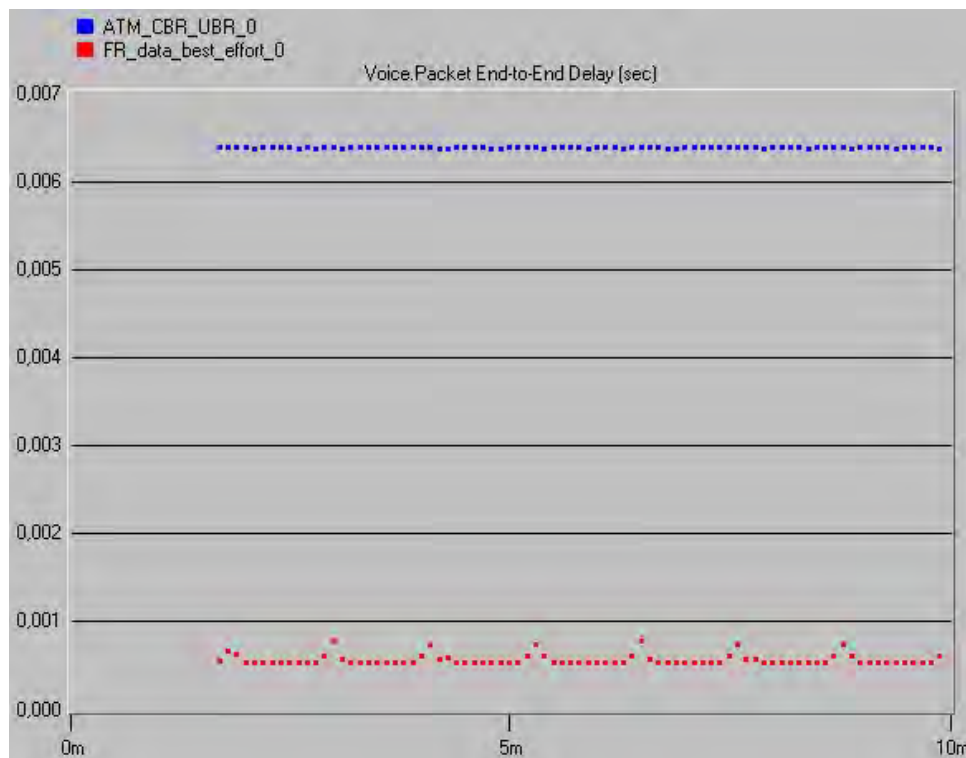
Obr. D.7: Kolísání zpoždění pro hlasovou aplikaci pro scénáře se zvýšenou zátěží u datových aplikací v s/min.

## D.2 Úkol 2

Druhý úkol je zaměřen na technologii Frame Relay. Pro tuto technologii je typické, že se před vlastním přenosem dat musí vytvořit virtuální okruh. Virtuální okruhy mohou být dvojího typu. V této laboratorní úloze jsou konfigurovány pouze trvalé virtuální okruhy PVC.

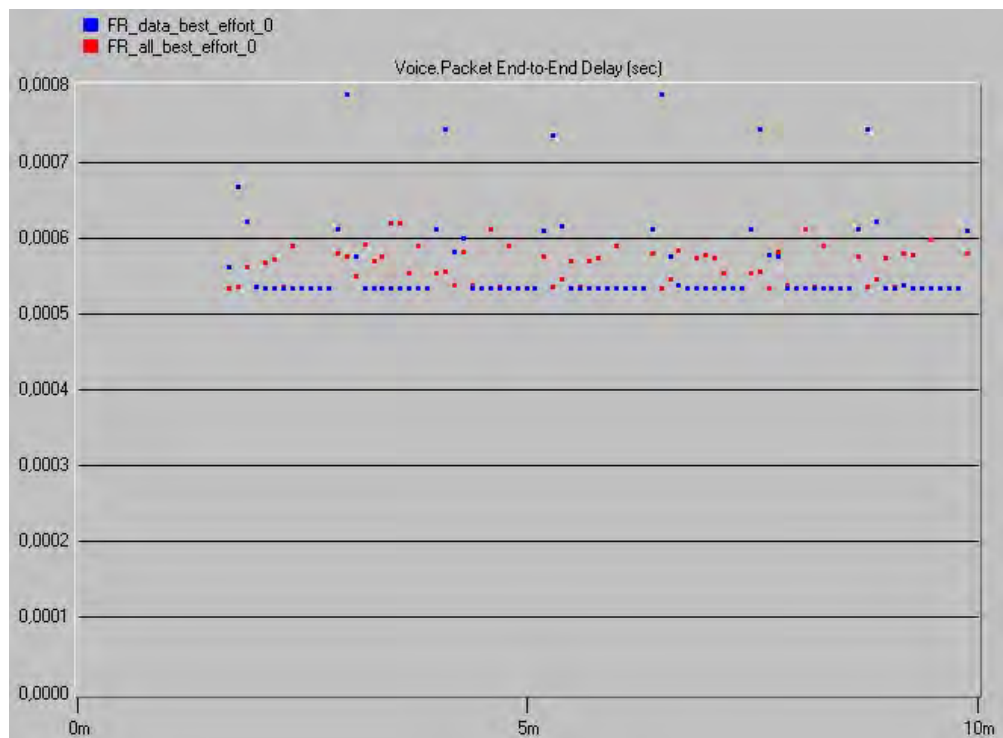
Doplňující otázky a úkoly:

- 1) Ze statistiky (Obr. D.8) vyplývá, že u technologie ATM při nastavené třídě služeb CBR má křivka konstantní průběh a ostatní aplikace při tomto vytížení sítě na ní nemají vliv, zatímco pro ToS *Interactive Voice* u technologie Frame Relay má vliv na hlasovou aplikaci i mírné zatížení sítě ostatními aplikacemi.

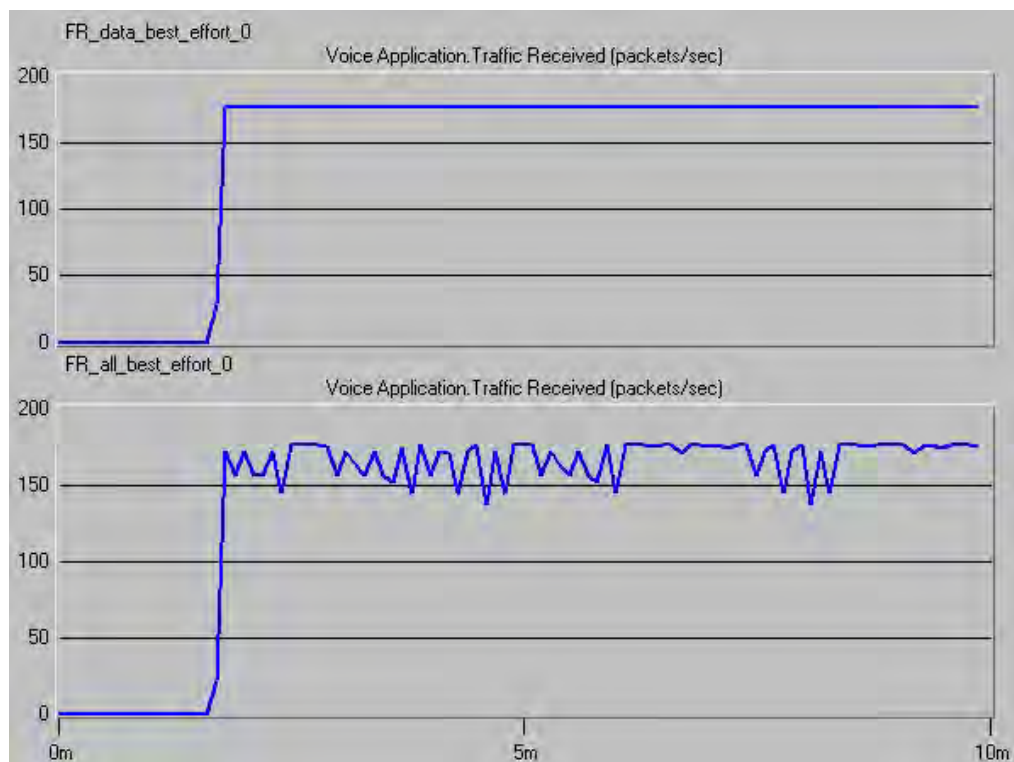


Obr. D.8: Zpoždění pro hlasovou aplikaci pro scénáře ATM a Frame Relay v s/min.

- 2) Ze statistiky (Obr. D.9) je patrné, že ve scénáři, kde je pro hlasovou aplikaci nakonfigurován typ služby *Interactive Voice* (modrá křivka) jsou špičkové hodnoty zpoždění vyšší než v případě scénáře, kde je pro veškerý provoz nakonfigurován typ služby *Best Effort*. Z tohoto závěru by se mohlo zdát, že je typ služby *Best Effort* pro hlasová data vhodnější. Nahlédneme-li však do statistiky pro přijatá data jednotlivými bezdrátovými klienty, zjistíme, že u scénáře s nakonfigurovaným typem služby *Best Effort* se nepřenesou všechny pakety, což by mělo negativní vliv na kvalitu hovoru.



Obr. D.9: Zpoždění pro hlasovou aplikaci pro scénáře Frame Relay v s/min.



Obr. D.10: Doručená data pro hlasovou aplikaci v pakety/min.

### 3) ATM – 4 třídy služeb:

- CBR

- VBR
- ABR
- UBR

Frame Relay – 7 typů služeb ToS

- Best Effort (0)
- Background (1)
- Standard (2)
- Excellent Effort (3)
- Streaming Multimedia (4)
- Interactive Multimedia (5)
- Interactive Voice (6)
- Reserved (7)

## **E OBSAH PŘILOŽENÉHO CD**

Na přiloženém CD je kromě elektronické verze diplomové práce umístěn soubor s vytvořenými programy laboratorních úloh. Laboratorní úlohy byly navrhovány a odzkoušeny pro verzi programu OPNET IT Guru Academic Edition 9.1.A (Build 1999).

Soubor se zdrojovými kódy obsahuje 4 složky (pro každou úlohu samostatná). Obsah těchto složek je nutné zkopírovat do složky „op\_models“, která se defaultně nachází na disku C:\Users\jméno\_uživatele\op\_models.

Po spuštění prostředí OPNET IT Guru poté stačí vybrat položku z menu programu *File/Open...* a vybrat požadovaný projekt podle jeho názvu.